HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: CƠ SỞ AN TOÀN THÔNG TIN
MÃ HỌC PHẦN: INT1472

ĐỀ TÀI: Tìm hiểu về hệ thống phát hiện tấn công, xâm nhập OSSEC: Kiến trúc, Cài đặt, Cấu hình, Tạo luật, Xây dựng 3 kịch bản phát hiện tấn công.

Các sinh viên thực hiện:

B22DCAT165	Trần Minh Khôi
B22DCAT223	Đặng Văn Phúc
B22DCAT133	Trần Ngọc Huân
B22DCAT225	Nguyễn Việt Phương
B22DCAT253	Đinh Thị Thanh Tâm

Tên nhóm: 06

Tên lớp: D22-001

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HÀ NỘI 2024

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành
1	Tìm hiểu kiến trúc của OSSEC	Đặng Văn Phúc	26/9/2024
2	Tìm hiểu cài đặt OSSEC	Nguyễn Việt Phương	26/9/2024
3	Tìm hiểu cấu hình của OSSEC	Trần Ngọc Huân	26/9/2024
4	Tìm hiểu tạo luật của OSSEC	Đinh Thị Thanh Tâm	26/9/2024
5	Xây dựng 3 kịch bản phát hiện tấn công	Trần Minh Khôi	26/9/2024

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Trần Minh Khôi	5	4	4	4	4
2	Đặng Văn Phúc	5	4	4	4	3
3	Nguyễn Việt Phương	5	4	4	4	3
4	Trần Ngọc Huân	5	4	4	4	3
5	Đinh Thị Thanh Tâm	5	4	4	4	3

Ghi chú:

- Thái độ tham gia: Đánh giá điểm thái độ tham gia công việc chung của nhóm (từ 0: không tham gia, đến 5: chủ động, tích cực).
- Mức hoàn thành CV: Đánh giá điểm mức độ hoàn thành công việc được giao (từ 0: không hoàn thành, đến 5: hoàn thành xuất sắc).
- Kỹ năng giao tiếp: Đánh giá điểm khả năng tương tác, giao tiếp trong nhóm (từ 0: không hoặc giao tiếp rất yếu, đến 5: giao tiếp xuất sắc).
- Kỹ năng hợp tác: Đánh giá điểm khả năng hợp tác, hỗ trợ lẫn nhau, giải quyết mâu thuẫn, xung đột
- Kỹ năng lãnh đạo: Đánh giá điểm khả năng lãnh đạo (từ 0: không có khả năng lãnh đạo, đến 5: có khả năng lãnh đạo tốt, tổ chức và điều phối công việc trong nhóm hiệu quả).

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
IDS	Intrusion Detection System	Hệ thống giúp phát hiện các hành động bất thường hoặc có dấu hiệu tấn công vào hệ thống mạng hoặc máy tính
HIDS	Host-based Intrusion Detection System	Là hệ thống phát hiện lỗ hổng (IDS) được cài dặt trên các máy tính hoặc các hệ thống máy chủ để giám sát hoạt động và phát hiện các hoạt động động thái bất thường hoặc gian lận
SIM	Security Information Management	Là một phần của hệ thống quản lý an ninh thông tin, thường chủ yếu tập trung vào việc thu thập , lưu trữ và quản lý thông tin bảo mật từ các hệ thống khác nhau
SEM	Security Event Management	Là một phần của hệ thống quản lý an ninh thông tin, thường chủ yếu tập trung vào việc giảm sát và phân tích các sự kiện bảo mật trong thời gian thực
SSH	Secure Shell	Là một giao thức mạng mã hóa cho phép truyền thông an toàn giữa hai máy tính
TCP	Transmission Control Protocol	Là một trong những giao thức cốt lõi của bộ giao thức Internet(IP)
IP	Internet Protocol	Là một giao thức thuộc bộ giao thức TCP/IP, được sử dụng để truyền dữ liệu qua mạng
FTP	File Transfer Protocol	Là một giao thức mạng tiếu chuẩn được sử dụng để truyền tải tệp tin giữa hai máy tính qua mạng TCP/IP, như Internet
CPU	Central Processing Unit	Là bộ xử lý trung tâm của máy tính, thường được ví như “bộ não” của hệ thống máy tính

LỜI MỞ ĐẦU

Cùng với sự phát triển mạnh mẽ của nền kinh tế toàn cầu, Internet ra đời, đơn giản hóa những cách thức chúng ta tương tác kinh doanh và truyền thông. Internet đã và đang thay đổi mọi quan niệm về Internet trở thành một đứa con đẻ của thời đại mới – thời đại công nghệ số. Internet tạo nên môi trường kinh doanh xóa đi mọi rào cản quốc gia và tạo ra một thị trường lớn nhất trong lịch sử nhân loại, cùng với đó là sự phát triển như vũ bão của mạng toàn cầu tại Việt Nam.

Bên cạnh những thành tựu to lớn mà mạng Internet mang lại cho nhân loại, vấn đề an toàn thông tin ngày càng được quan tâm hơn. Hàng ngày chúng ta được nghe rất nhiều thông tin về các cuộc tấn công vào các hệ thống thông tin quan trọng với những thiệt hại rất lớn về tài chính, thông tin riêng tư của các cá nhân và các tổ chức. Mục tiêu của các cuộc tấn công mạng thì rất đa dạng, từ những vấn đề cá nhân, những mục đích xấu trong kinh doanh cho đến mục tiêu chính trị với tầm ảnh hưởng trên nhiều quốc gia. Tội phạm an ninh mạng ngày càng phát triển cả về số lượng, quy mô và mức độ, khiến công ty hay tổ chức đặt lên hàng đầu.

Với khả năng kết nối nhiều máy tính và mạng, bảo mật trở thành vấn đề lớn và khó khăn hơn bao giờ hết trong môi trường doanh nghiệp. Hacker và những kẻ xấu luôn tìm cách khai thác những lỗ hổng trong hệ thống mạng và dịch vụ web. Rất nhiều hãng có uy tín về bảo mật đã có nhiều giải pháp để hạn chế sự tấn công trên mạng và những phương thức đã được triển khai trong nỗ lực bảo vệ hạ tầng mạng và truyền thông qua mạng internet bao gồm firewall, các phương thức mã hóa, và các mạng riêng ảo,...

Phát hiện xâm nhập cũng là một kỹ thuật liên quan được áp dụng. Các phương thức phát hiện xâm nhập xuất hiện vài năm gần đây. Với các phương pháp này người quản trị có thể thu thập và sử dụng thông tin từ các dạng tấn công chưa được biết hoặc phát hiện cuộc tấn công đang diễn ra. Những thông tin thu thập được sẽ giúp người quản trị gia cố an ninh mạng, đưa ra các chính sách an toàn cho hệ thống nhằm giảm thiểu những tấn công bất hợp pháp.

Vì vậy, là những sinh viên được trang bị những kiến thức của ngành an toàn thông tin với những kiến thức đã được tiếp thu, nên nhóm chúng em đã chọn đề tài "**Tìm hiểu về hệ thống phát hiện tấn công, xâm nhập OSSEC**" để thực hiện bài tập lớn với mục đích tìm hệ thống phát hiện và phòng chống xâm nhập trái phép nhằm đảm bảo an toàn hệ thống mạng.

Báo cáo bài tập lớn gồm 3 chương với nội dung chính như sau:

- Chương 1 nghiên cứu tổng quan về hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS), bao gồm các nội dung khái quát về các thành phần, chức năng , nguyên lý hoạt động của hệ thống phát hiện xâm nhập và phân loại các hệ thống phát hiện xâm nhập.
- Chương 2 đi sâu vào tìm hiểu hệ thống phát hiện xâm nhập OSSEC HIDS, bao gồm các nội dung về kiến trúc, tạo luật, thực hiện việc cài đặt và cấu hình OSSEC trên Linux và Windows.
- Chương 3 là xây dựng 3 kịch bản phát hiện tấn công của OSSEC bao gồm: phát hiện tấn công Brute-Force SSH, phát hiện dò quét cổng Port-Scanning và phát hiện Rootkit.

CHƯƠNG 1. TỔNG QUAN VỀ HỆ THỐNG PHÁT HIỆN XÂM NHẬP

1.1 Hệ thống phát hiện xâm nhập (IDS)

Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) là hệ thống phần cứng hoặc phần mềm có chức năng tự động theo dõi các sự kiện sảy ra, giám sát lưu thông mạng, và cảnh báo các hoạt động khả nghi cho người quản trị.

Một hệ thống IDS có thể vừa là phần cứng vừa là phần mềm phối hợp một cách hợp lí để nhận ra những mối nguy hại có thể tấn công. Chúng phát hiện những hoạt động xâm nhập trái phép vào mạng. Chúng có thể xác định những hoạt động xâm nhập bằng việc kiểm tra sự đi lại của mạng, những host log, những system call, và những khu vực khác khi phát ra những dấu hiệu xâm nhập.

IDS cũng có thể phân biệt giữa tấn công từ bên trong hay tấn công từ bên ngoài. IDS phát hiện dựa trên các dấu hiệu đặc biệt về nguy cơ đã biết (giống như phần mềm diệt virus dựa vào dấu hiệu đặc biệt phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đạc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường.

1.1.1 Chức năng của hệ thống phát hiện xâm nhập

Hệ thống phát hiện xâm nhập cho phép các tổ chức bảo vệ hệ thống của họ khỏi những đe dọa với việc gia tăng kết nối mạng và sự tin cậy của hệ thống thông tin. Những đe dọa đối với an ninh mạng ngày càng trở nên cấp thiết đã đặt ra câu hỏi cho các nhà an ninh mạng chuyên nghiệp có nên sử dụng hệ thống phát hiện xâm nhập trừ khi những đặc tính của hệ thống phát hiện xâm nhập là hữu ích cho họ, bổ sung những điểm yếu của hệ thống khác.

Những chức năng quan trọng nhất của IDS chính là:

- Giám sát: Lưu lượng mạng và các hoạt động khả nghi.
- Cảnh báo: Báo cáo về tình trạng mạng cho hệ thống và quản trị viên.
- Bảo vệ: Dùng những thiết lập mặc định và các cấu hình từ nhà quản trị để có những hành động thiết thực chống lại kẻ xâm nhập và phá hoại.

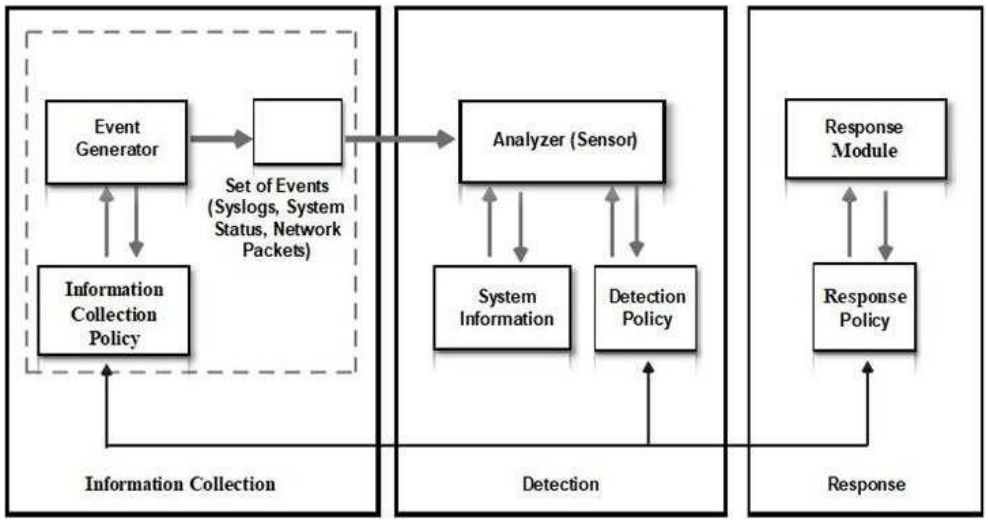
Ngoài ra, có những chức năng mở rộng như:

- Phân biệt: Tấn công từ bên trong và tấn công từ bên ngoài.

- Phát hiện: Những dấu hiệu bất thường dựa trên những gì đã biết hoặc nhở. vào sự so sánh thông lượng mạng hiện tái với Baseline.

Khi IDS chạy một thời gian sẽ đưa ra được những điểm yếu đó là điều hiển nhiên. Việc đưa ra những điểm yếu đó nhằm đánh giá chất lượng việc thiết kế mạng cũng như cách bố trí bảo vệ phòng thủ của các nhà quản trị mạng.

1.1.2 Các thành phần của hệ thống phát hiện xâm nhập



Hình 1 - Các thành phần của IDS

Kiến trúc của một hệ thống IDS bao gồm các thành phần chính sau: Thành phần thu thập gói tin (Information Collection), thành phần phân tích gói tin (Detection) và thành phần phản hồi (Respotion). Trong ba thành phần này, thành phần phân tích gói tin là quan trọng nhất và bộ cảm biến (sensor) đóng vai trò quan quyết định nên cần được phân tích để hiểu rõ hơn về kiến trúc của một hệ thống phát hiện xâm nhập.

Ở thành phần phân tích gói tin này bộ cảm biến đóng vai trò quyết định. Bộ cảm biến tích hợp với thành phần là sưu tập dữ liệu và một bộ tạo sự kiến. Cách sưu tập này được xác định bởi chính sách tạo sự kiện để định nghĩa chế độ lọc thông tin sự kiện. Vai trò của bộ cảm biến là dùng để lọc thông tin và loại bỏ dữ liệu không tương thích đạt được từ các sự kiện liên quan với hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động nghi ngờ. Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện cho mục này. Ngoài ra còn có các thành phần: dấu hiệu tấn công, profile hành vi thông thường, các tham số cần thiết. Thêm vào đó, cơ sở dữ liệu giữa các tham số cấu hình, gồm các chế độ truyền thông với module đáp trả. Bộ cảm biến cũng có sơ sở dữ liệu của riêng nó.

1.1.3 Nguyên lý hoạt động của hệ thống phát hiện xâm nhập

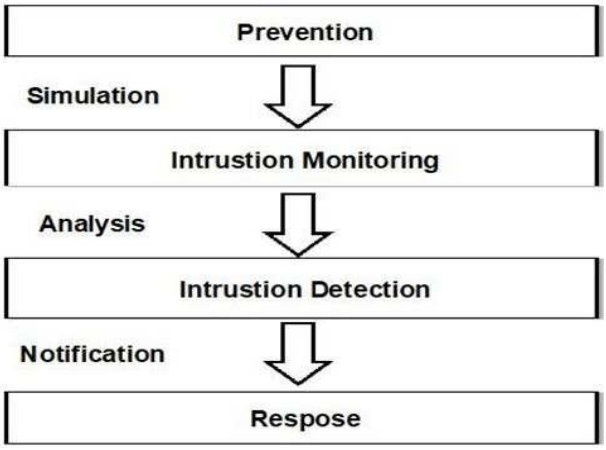
Quá trình phát hiện có thể được mô tả bởi các yếu tố nền tảng cơ bản sau:

- **Thu thập thông tin (Infotmation Source):** kiểm tra tất cả các gói tin trên mạng (Information Monitoring).
- **Sự phân tích (Analysis):** phân tích tất cả các gói tin đã thu thập để cho biết hành động nào là tấn công (Intruction Detection).
- **Xuất thông tin cảnh báo (Response):** hành động cảnh báo cho sự tấn công được phân tích ở trên nhờ bộ phận thông báo (Notification).

Khi một hành động xâm nhập được phát hiện, IDS đưa ra các cảnh báo đến các quản trị viên hệ thống về sự việc này. Bước tiếp theo được thực hiện bởi các quản trị hoặc có thể là bản thân IDS bằng cách lợi dụng các tham số đo bổ sung (các chức năng khóa để giới hạn các session, backup hệ thống, định tuyến các kết nối đến bẫy hệ thống, cơ sở hạ tầng hợp lệ,…) theo các chính sách bảo mật của các tổ chức. Một IDS là một thành phần nằm trong chính sách bảo mật.

Giữa các nhiệm vụ IDS khác nhau, việc nhận ra kẻ xâm nhập là một trong những nhiệm vụ cơ bản. Nó cũng hữu dụng trong việc nghiên cứu mang tính pháp lý các tình tiết và việc cài đặt các bản vá thích hợp để cho phép phát hiện các cuộc tấn công trong tương lai nhằm vào các cá nhân cụ thể hoặc tài nguyên hệ thống.

Phát hiện xâm nhập đôi khi có thể đưa ra các cảnh báo sai, ví dụ vấn đề xảy ra do trục trặc về giao diện mạng hoặc việc gửi phần mô tả các cuộc tấn công hoặc các chữ ký thông qua email.



Hình 2 - Hoạt động của IDS

Hầu hết các công cụ phát hiện xâm nhập trái phép là thụ động, khi phát hiện được cuộc tấn công tạo ra cảnh báo nhưng không thực hiện biện pháp đối phó. Đòi hỏi người quản trị trực tiếp kiểm tra cảnh báo và thực hiện hành động phù hợp. Điều này có thể gây chậm trễ trong việc xử lý với các cuộc tấn công.

Có một số IDS có khả năng thực hiện hành động như thay đổi trạng thái bảo mật để phản ứng lại với những cuộc tấn công. Các IDS này có thể thay đổi quyền của file, đặt thêm luật của tường lửa, ngừng tiến trình hay ngắt kết nối. Những hệ như vậy có hiệu quả rất lớn, nhưng cũng có thể bị kẻ tấn công lợi dụng để tự gây hại cho hệ, hay gây từ chối dịch vụ.

1.2 Phân loại hệ thống phát hiện xâm nhập

1.2.1 Host-base IDS (HIDS)

Những hệ thống HIDS được cài đặt như là những agent (tác nhân) trên một host, kiểm soát lưu lượng vào ra trên một máy tính, có thể được triển khai trên nhiều máy tính trong hệ thống mạng. HIDS thường được đặt trên các host xung yếu của tổ chức, và các server trong vùng DMZ - thường là mục tiêu bị tấn công đầu tiên.

Bằng cách cài đặt một IDS trên máy tính chủ, ta có thể quan sát tất cả những hoạt động hệ thống, như các file log những thông điệp báo lỗi trên hệ thống máy chủ và những lưu lượng mạng thu thập được. Trong khi những đầu dò của mạng có thể phát hiện một cuộc tấn công, thì chỉ có hệ thống dựa trên máy chủ mới có thể xác định xem cuộc tấn công có thành công hay không. Thêm nữa là, hệ thống dựa trên máy chủ có thể ghi nhận những việc mà người tấn công đã làm trên máy chủ bị tấn công (compromised host).

Nhiệm vụ chính của HIDS là giám sát các thay đổi trên hệ thống, bao gồm (not all):

- Các tiến trình.
- Các entry của Registry.
- Mức độ sử dụng CPU.
- Kiểm tra tính toàn vẹn và truy cập trên hệ thống file.
- Một vài thông số khác.

Các thông số này khi vượt qua một ngưỡng định trước hoặc những thay đổi khả nghi trên hệ thống file sẽ gây ra báo động.

Ưu điểm của HIDS:

- Có khả năng xác định người dung liên quan tới một sự kiện.
- Hids có khả năng phát hiện các cuộc tấn công diễn ra trên một máy.
- Có thể phân tích các dữ liệu mã hóa.
- Cung cấp các thông tin về host trong lúc tấn công diễn ra.

Nhược điểm HIDS:

- Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.
- Khi hệ điều hành bị hạ do tấn công, đồng thời HIDS cũng bị hạ.
- Hids phải được thiết lập trên từng host giám sát
- Hids không có khả năng phát hiện các cuộc dò mạng.
- Hids cần tài nguyên Host để hoạt động.
- Đa số chạy trên hệ điều hành window. Tuy nhiên cũng đã có 1 số chạy trên linux chặng hạng Ubuntu.

1.2.2 Network-base IDS (NIDS)

NIDS được đặt giữa kết nối hệ thống mạng bên trong và mạng bên ngoài để giám sát toàn bộ lưu lượng vào ra. Có thể là một thiết bị phần cứng riêng biệt được thiết lập sẵn hay phần mềm cài đặt trên máy tính (Snort).

NIDS sử dụng bộ dò và bộ bộ cảm biến cài đặt trên toàn mạng. Những bộ dò này theo dõi trên mạng nhằm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa hay là những dấu hiệu. Những bộ bộ cảm biến thu nhận và phân tích lưu lượng trong thời gian thực. Khi ghi nhận được một mẫu lưu lượng hay dấu hiệu, bộ cảm biến gửi tín hiệu cảnh báo đến trạm quản trị và có thể được cấu hình nhằm tìm ra biện pháp ngăn chặn những xâm nhập xa hơn. NIDS là tập nhiều sensor được đặt ở toàn mạng để theo dõi những gói tin trong mạng so sánh với với mẫu đã được định nghĩa để phát hiện đó là tấn công hay không.

Ưu điểm của NIDS

- Quản lý được một phân đoạn mạng (network segment).
- Trong suốt với người sử dụng và kẻ tấn công.
- Cài đặt và bảo trì đơn giản, không làm ảnh hưởng đến mạng.
- Tránh được việc bị tấn công dịch vụ đến một host cụ thể.
- Có khả năng xác định được lỗi ở tầng network.
- Độc lập với hệ điều hành.

Hạn chế của NIDS

- Có thể xảy ra trường hợp báo động giả, tức là không có dấu hiệu bất thường mà IDS vẫn báo.
- Không thể phân tích được các lưu lượng đã được mã hóa như SSH, IPSec, SSL,…
- NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả.
- Không thể cho biết việc mạng bị tấn công có thành công hay không, để người quản trị tiến hành bảo trì hệ thống.

Một trong những hạn chế là giới hạn băng thông. Những bộ thu thập dữ liệu phải thu thập tất cả lưu lượng mạng, sắp xếp lại và phân tích chúng. Khi tốc độ mạng tăng lên thì khả năng của bộ thu thập thông tin cũng vậy. Một giải pháp là phải đảm bảo cho mạng được thiết kế chính xác.

Một cách mà hacker cố gắng che đậy cho hoạt động của họ khi gặp các hệ thống IDS là phân mảnh dữ liệu gói tin. Mỗi giao thức có một kích cỡ gói dữ liệu có hạn, nếu dữ liệu truyền qua mạng truyền qua mạng lớn hơn kích cỡ này thì dữ liệu bị phân mảnh. Phân mảnh đơn giản là quá trình chia nhỏ dữ liệu. Thứ tự sắp xếp không thành vấn đề miễn là không bị

chồng chéo dữ liệu, bộ cảm biến phải tái hợp lại chúng.

Hacker cố gắng ngăn chặn phát hiện bằng cách gởi nhiều gói dữ liệu phân mảnh chồng chéo. Một bộ cảm biến không phát hiện được các hoạt động xâm nhập nếu không sắp xếp gói tin lại một cách chính xác.

1.2.3 So sánh HIDS và NIDS

Trong phần trước đã nói sơ lược về khái niệm Host-based IDS (HIDS) và Network-based IDS (NIDS). Trong phần này sẽ cho chúng ta cái nhìn cụ thể về những điểm mạnh, yếu của chúng, có một điểm chung của các IDS là bản thân nó không tự chống các cuộc tấn công hoặc ngăn chặn những khai thác lỗi thành công, thực tế thì IDS chỉ cho chúng ta biết mạng đang bị nguy hiểm và giá trị chính của nó là cho biết điều gì sắp xảy ra, giúp cho người quản trị có những chính sách hợp lý cho mạng và cho host.

Bảng dưới đây sẽ cho ta cái nhìn trực quan hơn về HIDS và NIDS:

CHỨC NĂNG	HIDS	NIDS	ĐÁNH GIÁ
Bảo vệ trong mạng LAN	*****	*****	Cả hai đều bảo vệ được mạng LAN
Bảo vệ ngoài mạng LAN	*****		Chỉ có HIDS
Dễ dàng cho việc quản trị	*****	*****	Tương đương như nhau xét về bối cảnh quản trị chung
Tính linh hoạt	*****	**	HIDS có tính linh hoạt cao hơn
Giá thành	***	*	HIDS là hệ thống ưu tiên tiết kiệm hơn nếu chọn đúng sản phẩm
Dễ dàng trong việc bổ sung	****	****	Cả hai tương đương nhau
Đào tạo ngắn hạn cần thiết	****	**	HIDS yêu cầu việc đào tạo ít hơn
Băng tần cầu yêu cầu trong LAN	0	2	NIDS sử dụng băng tần LAN rộng còn HIDS thì không

Network overhead	1	2	NIDS cần 2 yêu cầu băng tần mạng đối với bất kì mạng LAN nào
Băng tần yêu cầu Internet	**	**	Cả hai đều cần băng tần Internet để cập nhật kịp thời các file mẫu
Các yêu cầu về cổng mở rộng		****	NIDS yêu cầu phải kích hoạt mở rộng cổng để đảm bảo lưu lượng LAN được quét
Chu kì nâng cấp cho các client	*****		HIDS nâng cấp cho tất cả các client với một file mẫu trung tâm
Khả năng thích nghi trong các nền ứng dụng	**	****	NIDS có khả năng thích nghi trong các nền ứng dụng hơn
Chế độ quét thanh ghi cục bộ	****		Chỉ có HIDS mới có thể thực hiện
Bản ghi	***	***	Cả hai hệ thống đều có chức năng bản ghi
Chức năng cảnh báo	***	***	Cả hau hệ thống đều có chức năng cảnh báo cho từng cá nhân và quảng trị viên
Loại bỏ gói tin		*****	Chỉ các tính năng NIDS mới có phương thức này
Kiến thức chuyên môn	***	*****	NIDS cần nhiều kiến thức chuyên môn hơn trong cài đặt và sử dụng
Quản lý tập trung	**	***	NIDS có chiếm ưu thế hơn
Khả năng vô hiệu hóa các hệ số rủi ro	*	****	NIDS có hệ số rủi ro nhiều hơn so với HIDS

Bảng 1 - Bảng so sánh giữa HIDS và NIDS

1.3 Mô hình triển khai IDS

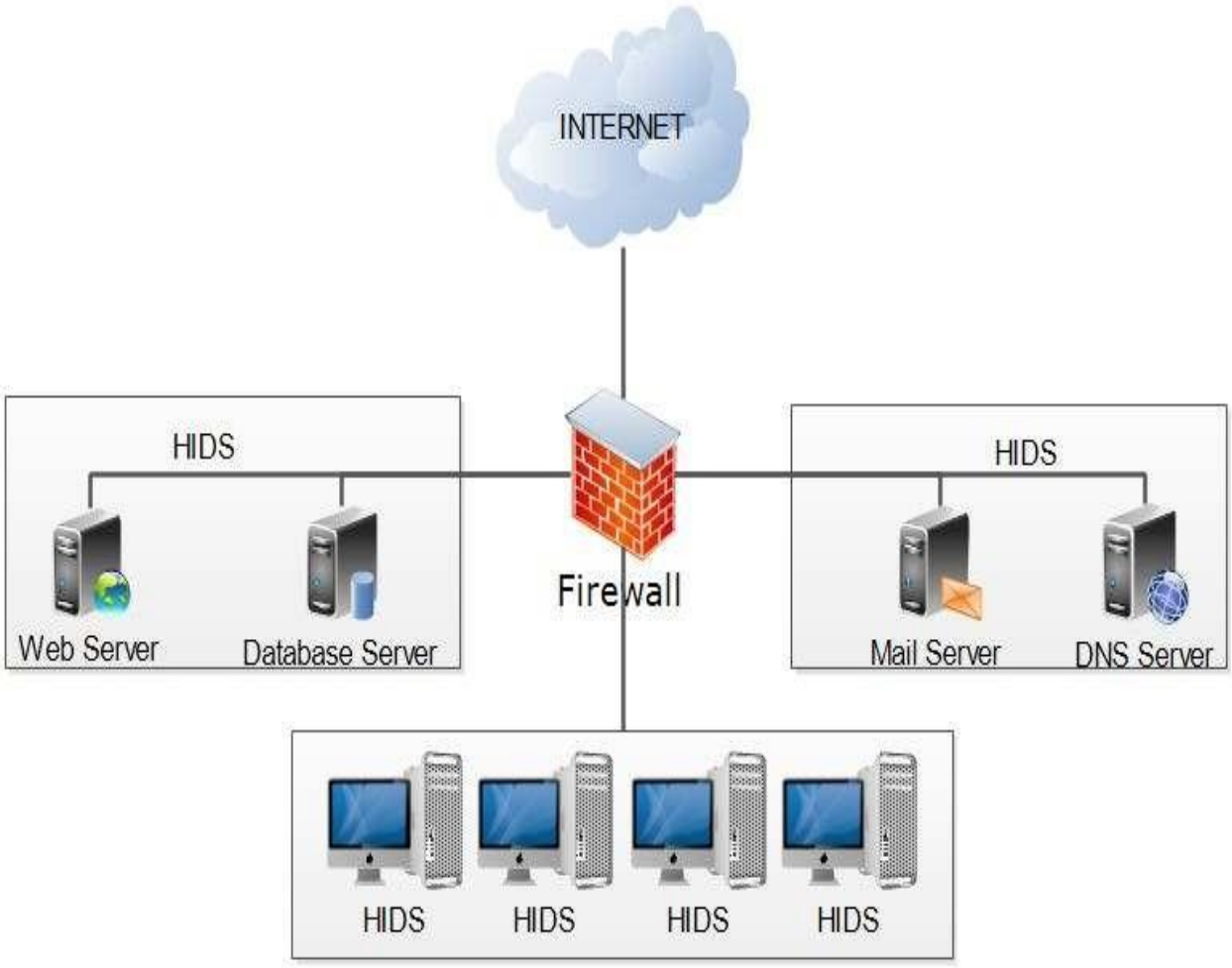
Phụ thuộc vào mô hình mạng, có thể đặt IDS ở một hoặc nhiều vị trí. Tùy thuộc vào loại xâm nhập muốn phát hiện, có thể là bên trong, bên ngoài, hoặc cả hai. Ví dụ, nếu cần phát hiện một tấn công từ bên ngoài, có một router kết nối ra Internet, thì nơi tốt nhất cần đặt IDS là nên trong Router hoặc tường lửa. Nếu bạn có nhiều đường ra Internet, bạn có thể cần mỗi IDS tại mỗi điểm kết nối đó. Tuy nhiên nếu cần phát hiện các nguy cơ từ bên trong, tốt nhất cần đặt IDS tại mỗi phân đoạn mạng (network segment).

1.3.1 Mô hình HIDS

HIDS có hai điểm khác biệt khi triển khai so với NIDS. HIDS chỉ theo dõi được host mà nó đang được cài đặt và card mạng hoạt động ở trạng thái bình thường là **non-promiscuous** (hay còn gọi là trạng thái active).

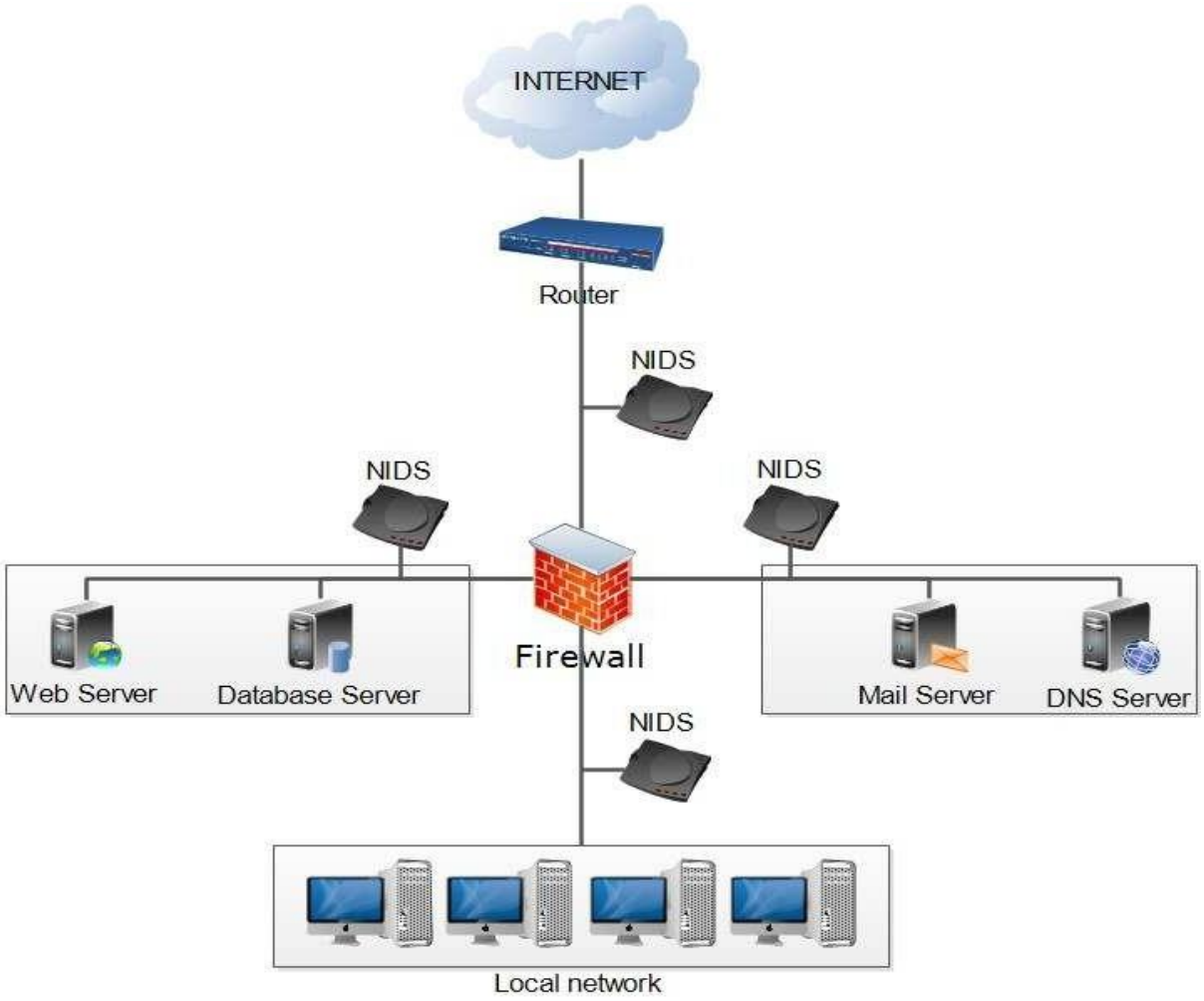
Khi triển khai theo mô hình HIDS có một số điểm thuận lợi như sau:

- Card mạng chỉ cần hoạt động ở chế độ bình thường nên không cần phải trang bị thêm card mạng mới, bởi vì không phải tất cả các card mạng đều có khả năng chuyển sang trạng thái promiscuos. Khi hoạt động ở chế độ bình thường sẽ không yêu cầu nhiều xử lý của CPU so với trạng thái promiscuous.
- Do chỉ theo dõi cho một host cụ thể nên HIDS có thể theo dõi sâu hơn về những thông tin của hệ thống như system calls, những thay đổi trong file hệ thống, system logs.
- Người quản trị có thể linh động cấu hình tập hợp các rule cho từng host cụ thể. Ví dụ như không cần phải sử dụng rule để phát hiện tấn công DNS(Domain Name System) trong khi một máy tính không chạy dịch vụ DNS. Do đó có thể giảm bớt những rule không cần thiết, giúp tăng cường hiệu suất và giảm thiểu những xử lý quá tải.



Hình 3 - Mô hình triển khai HIDS

1.3.2 Mô hình NIDS



Hình 4 - Mô hình triển khai NIDS

Không giống với HIDS, trong mô hình triển khai NIDS ở hình 4, NIDS theo dõi toàn bộ dữ liệu trên từng đoạn mạng mà nó được cài đặt. Trong mô hình trên sử dụng 4 NIDS để theo dõi luồng dữ liệu trên 4 đoạn mạng khác nhau là các public server và hệ thống mạng bên trong. Như đã nói trong các phần trước, đặc trưng của NIDS là làm sao để từng NIDS có thể theo dõi được tất cả các dữ liệu được trao đổi trên từng đoạn mạng. Do đó cần phải có một số yêu cầu đặc biệt về mặt kỹ thuật để triển khai NIDS:

Card mạng của NIDS cần phải hỗ trợ chế độ promiscuous để NIDS có thể nhận được các gói tin có destination MAC không gửi cho nó. Tuy nhiên đây chỉ là điều kiện cần để NIDS nhận được dữ liệu trên mạng, vấn đề chính là làm sao để toàn bộ dữ liệu trên đoạn mạng có thể đổ dồn vào NIDS.

Có một số giải pháp để giải quyết vấn đề giúp NIDS có thể bắt được toàn bộ dữ liệu trên đoạn mạng như: sử dụng Hub, Network Tap và công nghệ Switch Port Analyzer (SPAN) của Cisco.

1.4 Các phương pháp nhận diện của hệ thống phát hiện xâm nhập

Các hệ thống IDS thường dùng nhiều phương pháp nhận diện khác nhau, riêng rẽ hoặc tích hợp nhằm mở rộng và tăng cường độ chính xác nhận diện. Có thể chia làm ba phương pháp nhận diện chính là: Signature-base Detection, Anormaly-base Detection và Stateful Protocol Analysis.

1.4.1 Nhận diện dựa vào dấu hiệu (Signature-base Detection)

Signature-base Detection sử dụng phương pháp so sánh các dấu hiệu của đối tượng quan sát với các dấu hiệu của các mối nguy hại đã biết. Phương pháp này có hiệu quả với các mối nguy hại đã biết nhưng hầu như không có hiệu quả hoặc hiệu quả rất ít đối với các mối nguy hại chưa biết, các mối nguy hại sử dụng kỹ thuật lẩn tránh (evasion techniques), hoặc các biến thể. Signature-based Detection không thể theo vết và nhận diện trạng thái của các truyền thông phức tạp.

1.4.2 Nhận diện dựa vào sự bất thường (Abnormaly-base Detection)

Abnormaly-base Detection so sánh định nghĩa của những hoạt động bình thường và đối tượng quan sát nhằm xác định các độ lệch. Một hệ IDS sử dụng phương pháp Abnormaly-base Detection có các profiles đặc trưng cho các hành vi được coi là bình thường, được phát triển bằng cách giám sát các đặc điểm của hoạt động tiêu biểu trong một khoảng thời gian. Sau khi đã xây dựng được tập các profile này, hệ IDS sử dụng phương pháp thống kê để so sánh các đặc điểm của các hoạt động hiện tại với các ngưỡng định bởi profile tương ứng để phát hiện ra những bất thường.

Profile sử dụng bởi phương pháp này có 2 loại là static và dynamic:

- Static profile không thay đổi cho đến khi được tái tạo, chính vì vậy dần dần nó sẽ trở nên không chính xác, và cần phải được tái tạo định kỳ.
- Dynamic profile được tự động điều chỉnh mỗi khi có các sự kiện bổ sung được quan sát, nhưng chính điều này cũng làm cho nó trở nên dễ bị ảnh hưởng bởi các phép thử dùng kỹ thuật giấu (evasion techniques). Ưu điểm chính của phương pháp này là nó rất có

hiệu quả trong việc phát hiện ra các mối nguy hại chưa được biết đến.

1.4.3 Phân tích trạng thái của giao thức (Staful Protocol Analysis)

Phân tích trạng thái protocol là quá trình so sánh các profile định trước của hoạt động của mỗi giao thức được coi là bình thường với đối tượng quan sát từ đó xác định độ lệch. Khác với phương pháp Anomaly-base Detection, phân tích trạng thái protocol dựa trên tập các profile tổng quát cung cấp bởi nhà sản xuất theo đó quy định 1 protocol nên làm và không nên làm gì. "Stateful" trong phân tích trạng thái protocol có nghĩa là IDS có khả năng hiểu và theo dõi tình trạng của mạng, vận chuyển, và các giao thức ứng dụng có trạng thái. Nhược điểm của phương pháp này là chiếm nhiều tài nguyên do sự phức tạp trong việc phân tích và theo dõi nhiều phiên đồng thời. Một vấn đề nghiêm trọng là phương pháp phân tích trạng thái protocol không thể phát hiện các cuộc tấn công khi chúng không vi phạm các đặc tính của tập các hành vi chấp nhận của giao thức.

1.5 Kết chương

Chương này đã giới thiệu khái quát về hệ thống phát hiện xâm nhập (IDS) đóng vai trò quan trọng trong việc bảo vệ an ninh mạng bằng cách giám sát, phát hiện và cảnh báo các hoạt động xâm nhập. Dù có thể chia thành HIDS và NIDS, mỗi loại có ưu, nhược điểm riêng và thích hợp cho các tình huống khác nhau. Trong khi HIDS tập trung bảo vệ từng máy chủ cụ thể và có khả năng phát hiện chi tiết, NIDS lại giám sát toàn bộ lưu lượng mạng, giúp phát hiện sớm các cuộc tấn công trên diện rộng. Tùy vào nhu cầu và cấu trúc mạng, việc lựa chọn hoặc kết hợp cả hai loại IDS sẽ tối ưu hóa bảo vệ hệ thống, đảm bảo an toàn thông tin trước các mối đe dọa mạng.

CHƯƠNG 2. ỨNG DỤNG HIDS OSSEC TRONG PHÁT HIỆN XÂM NHẬP

2.1 Giới thiệu

- OSSEC là một hệ thống phát hiện xâm nhập mã nguồn mở, chính xác là một HIDS (Host IDS). Thực hiện phân tích đăng nhập, kiểm tra tính toàn vẹn file, giám sát chính sách, phát hiện rootkit, thời gian thực cảnh báo và phản ứng tích cực. nó chạy trên hầu hết các hệ điều hành.

- OSSEC còn là một nền tảng đầy đủ để theo dõi và kiểm soát hệ thống của bạn. Nó trộn lẫn với nhau tất cả các khía cạnh của HIDS(dựa trên máy chủ phát hiện xâm nhập), giám sát đăng nhập và SIM/SIEM với nhau trong một giải pháp mã nguồn đơn giản, mạnh mẽ và cởi mở. Nó cũng được hỗ trợ và hỗ trợ đầy đủ bởi Trend Micro. OSSEC cho phép khách hàng cấu hình sự cố họ muốn được cảnh báo theo các mức ưu tiên khác nhau. Tích hợp SMTP, chúng ta có thể nhận được các thông báo cảnh báo của hệ thống qua email, tin nhắn. Ngoài ra, chúng ta có thể cấu hình, tùy chọn hoạt động phản ứng để ngăn chặn một cuộc tấn công có thể xảy ra.

2.2 Kiến trúc

OSSEC bao gồm nhiều phần. Nó có một Manager trung tâm để giám sát và nhận thông tin từ các Agent, syslog, cơ sở dữ liệu và từ các thiết bị Agentless.

2.2.1 Manager (or Server)

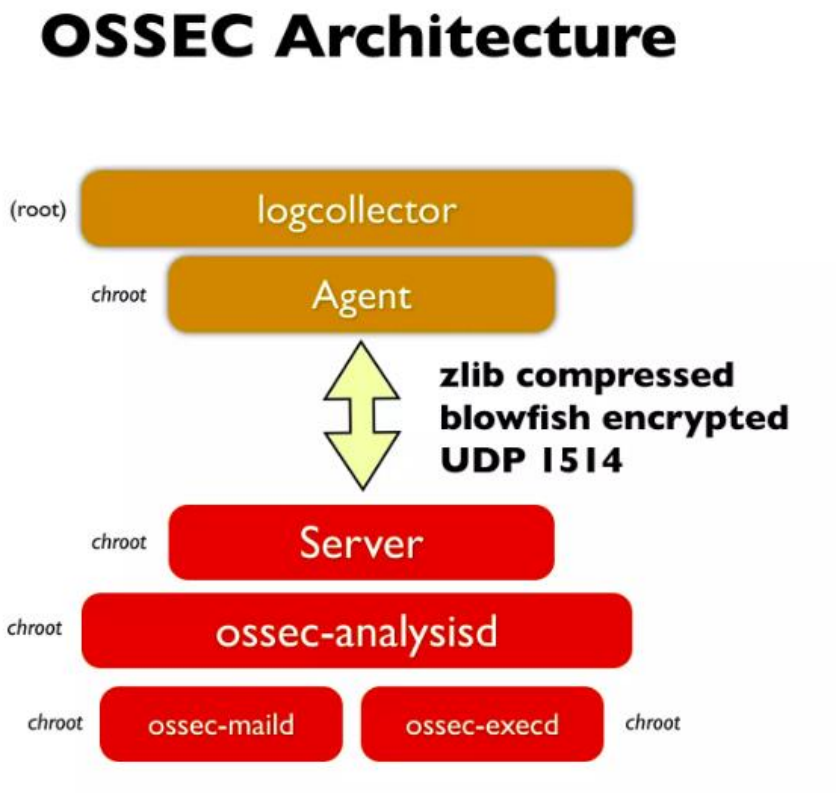
- Manager là phần trung tâm của triển khai OSSEC. Nó lưu trữ cơ sở dữ liệu kiểm tra tính toàn vẹn của tệp, nhật ký, sự kiện và mục nhập kiểm toán hệ thống. Tất cả các quy tắc, bộ giải mã và tùy chọn cấu hình chính được lưu trữ tập trung trong trình quản lý; giúp dễ dàng quản lý ngay cả một số lượng lớn tác nhân.

- Các tác nhân kết nối với máy chủ trên cổng 1514/udp. Phải cho phép giao tiếp với cổng này để các Agent có thể giao tiếp với máy chủ.

2.2.2 Agents

- Agent là một chương trình nhỏ hoặc tập hợp các chương trình, được cài đặt trên các hệ thống cần giám sát. Agent sẽ thu thập thông tin và chuyển tiếp đến người quản lý để phân tích và đối chiếu. Một số thông tin được thu thập theo thời gian thực, một số khác được thu thập theo định kỳ. Theo mặc định, nó có bộ nhớ và CPU rất nhỏ, không ảnh hưởng đến việc sử dụng hệ thống.

- Bảo mật Agent: Nó chạy với người dùng có đặc quyền thấp (thường được tạo trong quá trình cài đặt) và bên trong chroot jail bị cô lập khỏi hệ thống. Hầu hết cấu hình tác nhân có thể được đẩy từ trình quản lý. (chroot là viết tắt của change-root, chroot jail là một môi trường biệt lập nơi các chương trình chroot cư trú và được thực thi. Thuật ngữ chroot jail bắt nguồn từ khái niệm rằng quy trình và các quy trình con của nó bên trong môi trường chroot không có quyền truy cập hoặc được hiển thị với hệ thống tệp cơ sở và bị mắc kẹt trong giới hạn của chroot với các tài nguyên được xác định trước.)



Hình 5 - Sơ đồ kiến trúc của OSSEC(hệ thống HIDS)

2.2.3 Agentless

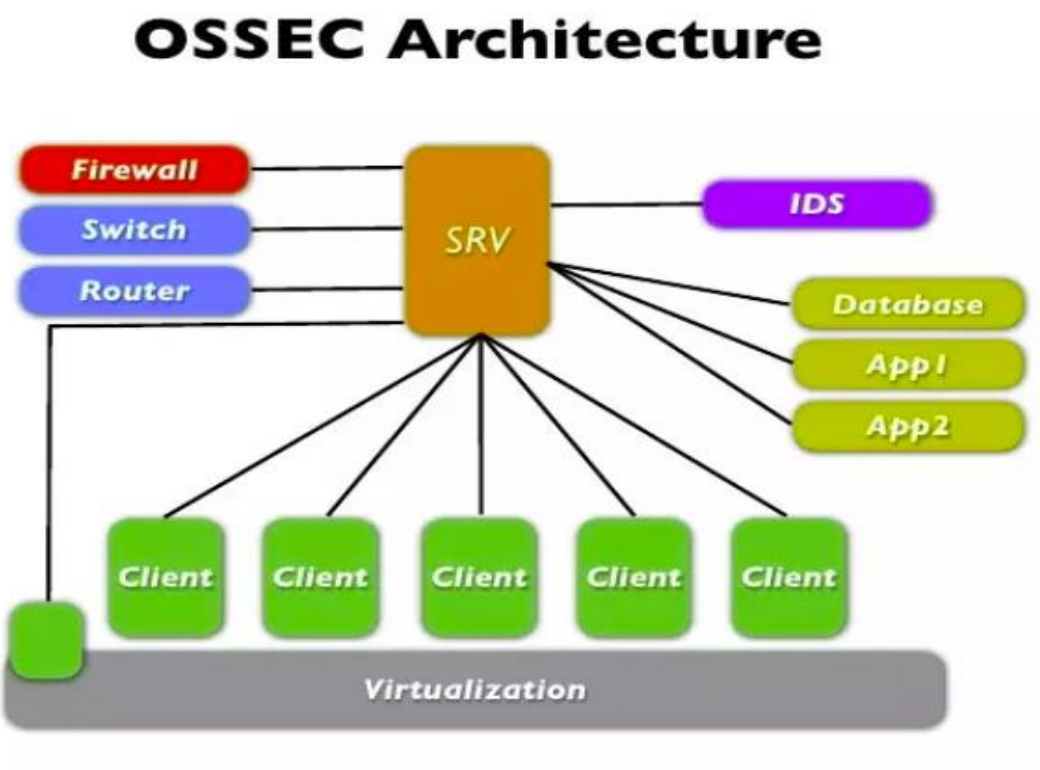
Đối với các hệ thống không thể cài đặt Agent, hỗ trợ không có tác nhân có thể cho phép thực hiện kiểm tra tính toàn vẹn. Rà soát Agentless có thể được sử dụng để giám sát tường lửa, bộ định tuyến và thậm chí cả hệ thống Unix.

2.2.4 Ảo hóa/VMWare

OSSEC cho phép bạn cài đặt Agent trên hệ điều hành khách. Nó cũng có thể được cài đặt bên trong một số phiên bản VMWare ESX, nhưng điều này có thể gây ra các vấn đề hỗ trợ. Với tác nhân được cài đặt bên trong VMware ESX, bạn có thể nhận được cảnh báo về thời điểm máy khách VM đang được cài đặt, xóa, khởi động, v.v. Nó cũng giám sát các lần đăng nhập, đăng xuất và lỗi bên trong máy chủ ESX. Ngoài ra, OSSEC thực hiện các kiểm tra Trung tâm bảo mật Internet (CIS) cho VMware, cảnh báo nếu có bất kỳ tùy chọn cấu hình không an toàn nào được bật hoặc bất kỳ vấn đề nào khác.

2.2.5 Firewalls, Switches và Routers

OSSEC có thể nhận và phân tích các sự kiện syslog từ nhiều loại tường lửa, bộ chuyển mạch và bộ định tuyến. Nó hỗ trợ tất cả các bộ định tuyến Cisco, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, tường lửa Netscreen, Checkpoint và nhiều loại khác.



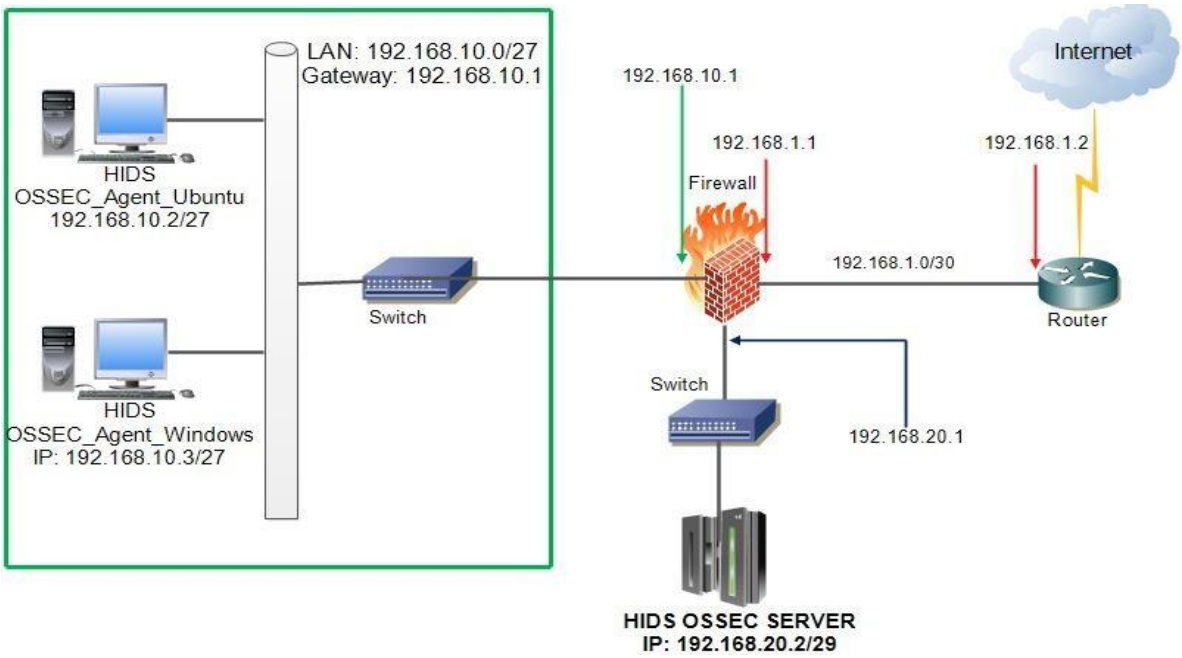
Hình 6 – OSSEC Network Architecture

Sơ đồ này cho thấy trình quản lý trung tâm nhận sự kiện từ các Agent và nhật ký hệ thống từ các thiết bị từ xa. Khi phát hiện ra điều gì đó, phản hồi chủ động có thể được thực hiện và quản trị viên sẽ được thông báo.

Hình 7 - OSSEC Server and Agent Architecture

2.3 Cài đặt và cấu hình hệ thống HIDS OSSEC

2.3.1 Mô hình triển khai



Hình 8 - Mô hình triển khai HIDS OSSEC

STT	HOSTNAME	IP	SUBNET MASK	GATEWAY
1	OSSEC Server	192.168.20.2	255.255.255.248	192.168.20.1
2	OSSEC_Agent_Ubuntu	192.168.10.2	255.255.255.224	192.168.10.1
3	OSSEC_Agent_Windows	192.168.10.3	255.255.255.224	192.168.10.1

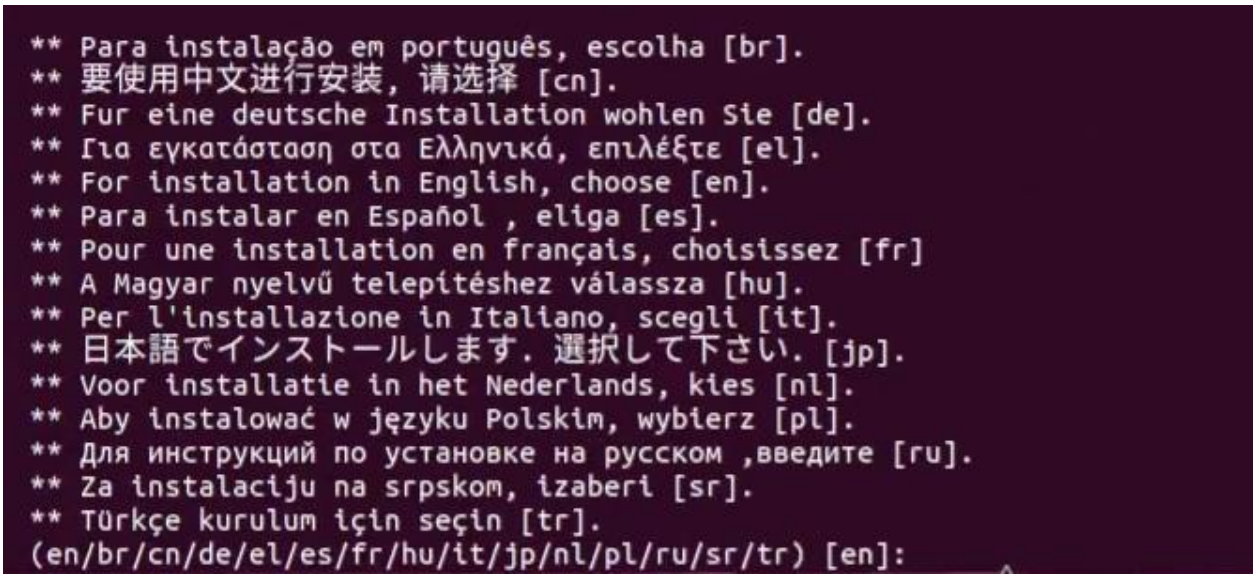
Bảng 2 - Mô tả IP mô hình triển khai

2.3.2 Triển khai OSSEC Server trên Ubuntu 22.04

Bước 1: OSSEC Server chạy trên nền tảng hệ điều hành Linux ở đây chúng ta sẽ triên khai OSSEC Server trên hệ điều hành Ubuntu, việc triển khai cài đặt không quá khó khăn tuy nhiên cần có cái gói cần cài đặt trước khi triển khai OSSEC để đảm bào hoạt động của OSSEC, chúng ta có thể cài đặt chúng qua lệnh sau:

- Cập nhật hệ thống**:** sudo apt update && sudo apt upgrade
- Cài đặt thành phần**:** sudo apt-get install build-essential make zlib1g-dev libpcre2-dev libevent-dev libssl-dev inotify-tools build-essential
- Chúng ta có thể download OSSEC từ trang chủ hoặc sử dụng câu lệnh :
wget https://github.com/ossec/ossec-hids/archive/refs/tags/3.7.0.tar.gz

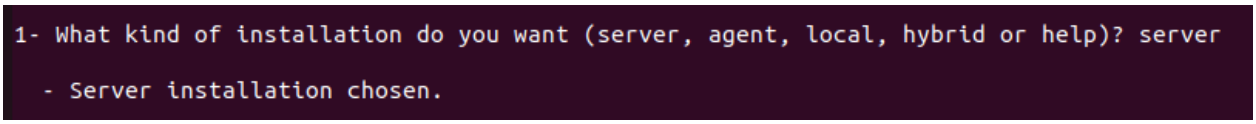
Bước 2: Sau khi download chúng ta tiến hành giải nén và vào thư mục để giải nén và chạy file **intall.sh**, giao diện cài đặt ngôn ngữ sẽ xuất hiện đầu tiên



Hình 9 - Cài đặt ngôn ngữ

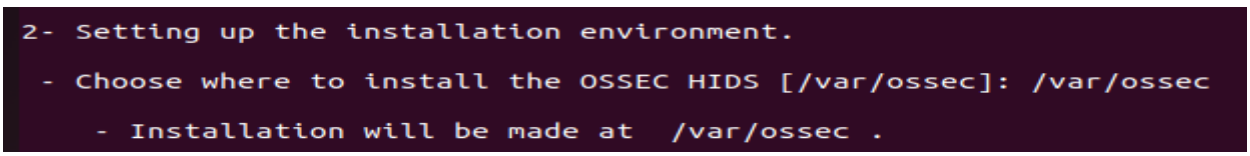
Bước 3: Tiếp sau đó chúng ta tiến hành lựa chọn các cấu hình ban đầu cho OSSEC sẽ có 3 phần bao gồm: Kiểu hoạt động sau khi cài đặt, vị trí thư mục cài đặt, cấu hình OSSEC HIDS

Đối với phần đầu tiên thì OSSEC sẽ hỏi ta về chế độ hoạt động, ta sẽ chọn server



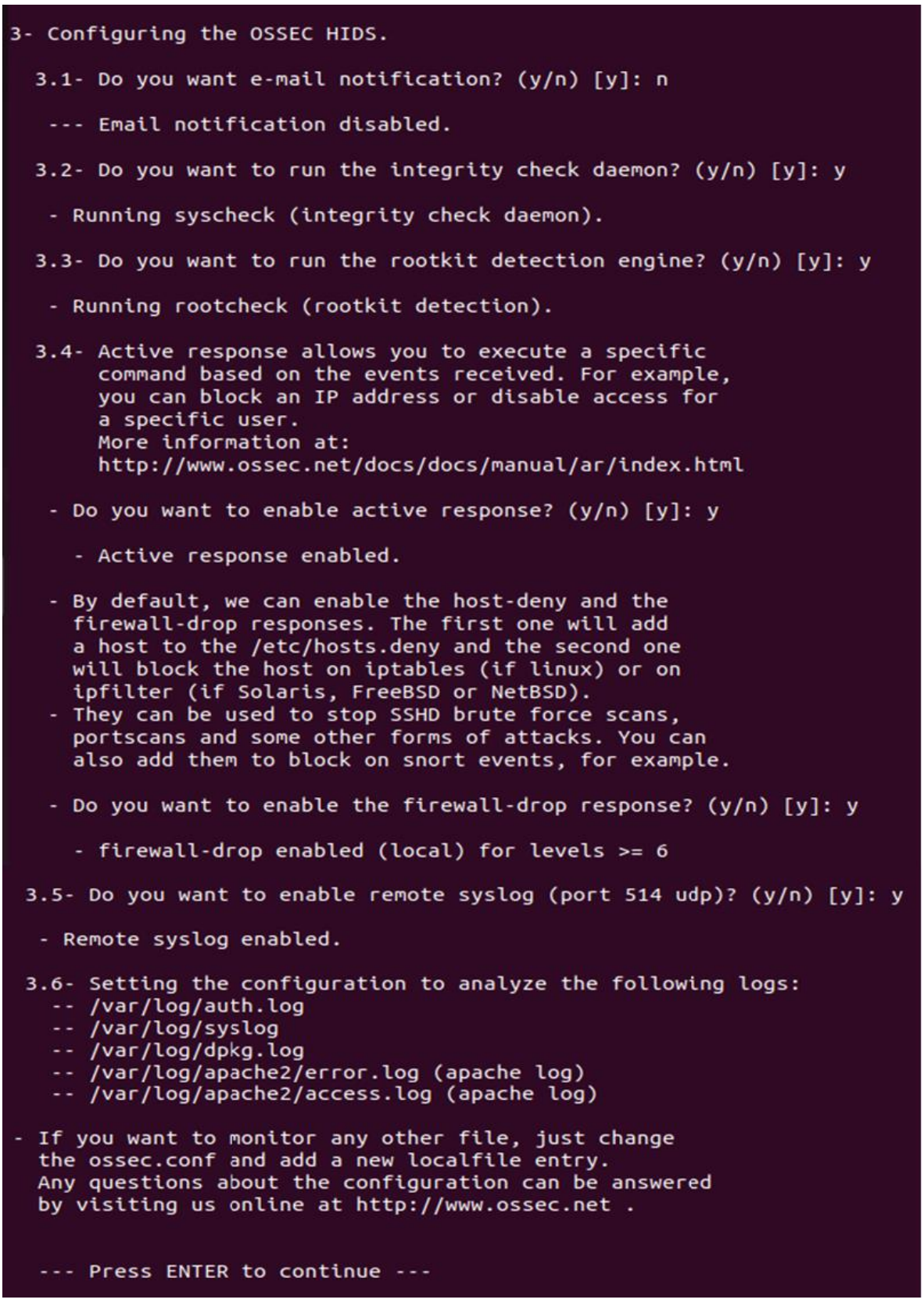
Hình 10 - Cài đặt chế độ hoạt động cho server

Đối với thư mục cài đặt mặc định sẽ được lưu ở /var/OSSEC nếu muốn thay đổi đường dẫn ta có thể có nhập đường dẫn khác vào hoặc có thể để mặc định và nhấn Enter>bỏ qua nó



Hình 11 - Cấu hình vị trí lưu OSSEC

Đối với phần cấu hình cho HIDS OSSEC ta có thể thiết lập như sau:



Hình 12 - Cấu hình HIDS OSSEC

Nhấn ENTER để hoàn tất thiết lập. Để khởi chạy ossec server dùng câu lệnh: sudo /var/ossec/bin/ossec-control start

```
root@ubuntu22:~/Ossec_src/ossec-hids-3.7.0# sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.7.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@ubuntu22:~/Ossec_src/ossec-hids-3.7.0#
```

Hình 13 - Khởi chạy OSSEC

Bước 4: Sau khi OSSEC được khởi động, chúng ta sẽ thêm các Agent cần quản lý vào Server, khởi chạy thực thi manage_agents trong (/var/OSSEC/bin) để thêm Agent chúng ta sẽ lựa chọn A.

```
root@ubuntu22:~# sudo /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

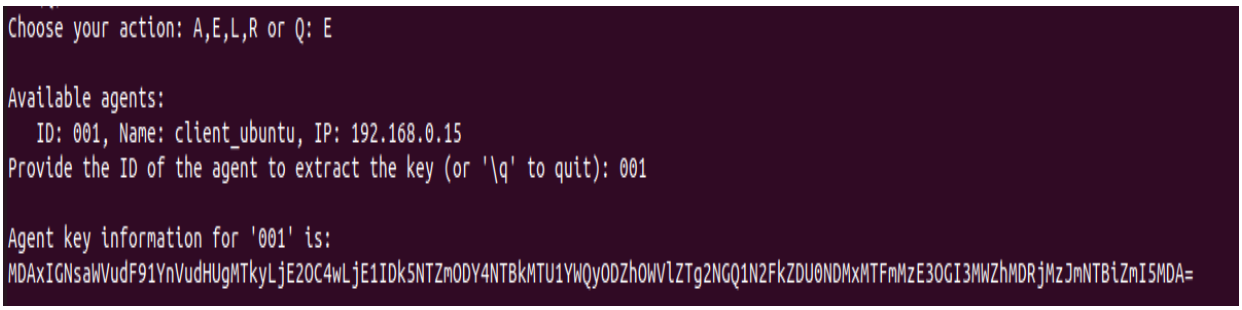
Hình 14 - Thêm Agent

Chúng ta nhập các thông tin về Agent theo yêu cầu

```
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: client_ubuntu
   * The IP Address of the new agent: 192.168.0.15
   * An ID for the new agent[001]: 001
Agent information:
   ID:001
   Name:client_ubuntu
   IP Address:192.168.0.15

Confirm adding it?(y/n): y
Agent added with ID 001.
```

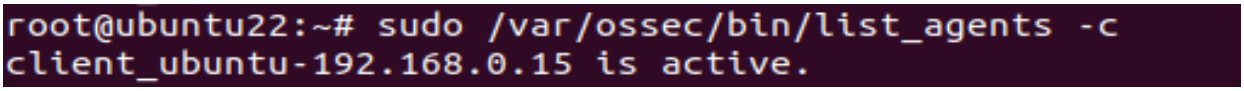
Hình 15 - Khai báo thông tin Agent

Sau đó chúng ta cần xác thực Agent vừa thêm vào với key, để thực hiện chúng ta quay về menu chính chọn E, sau đó nhập ID của Agent muốn xác thực vào, OSSEC sẽ cung cấp cho ta một key xác thực, ta sẽ dùng key này khi cài đặt OSSEC trên Agent



Hình 16 - Lấy key xác thực cho Agent

Chúng ta có thể kiểm tra tình trạng của agent xem đã kết nối với tới server được hay chưa bằng cách chạy lệnh thực thi list_agent -c trong file chứa lệnh thực thi var/OSSEC/bin/.



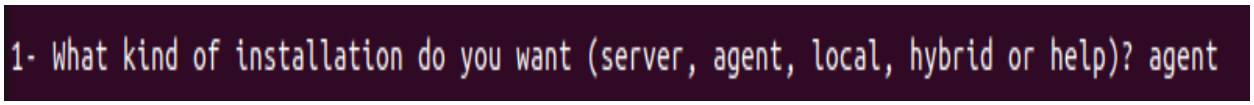
Hình 17 - Kiểm tra trạng thái Agent

Cần chú ý nếu trạng thái của agent không phải là Active, có thể là Disconnected hoặc Never Connect cần kiểm tra lại thông tin về agent đã khai báo trên server, kiểm tra xem OSSEC Agent đã được khởi động hay chưa, kiểm tra xem firewall trên server đã cho phép lưu lượng đi qua cổng 1514 udp hay chưa, nếu chưa cần phải mở cổng vì OSSEC sử dụng cổng 1514udp để kết nối với nhau.

2.3.3 Triển khai OSSEC Agent trên Ubuntu 22.04 và Windows 7

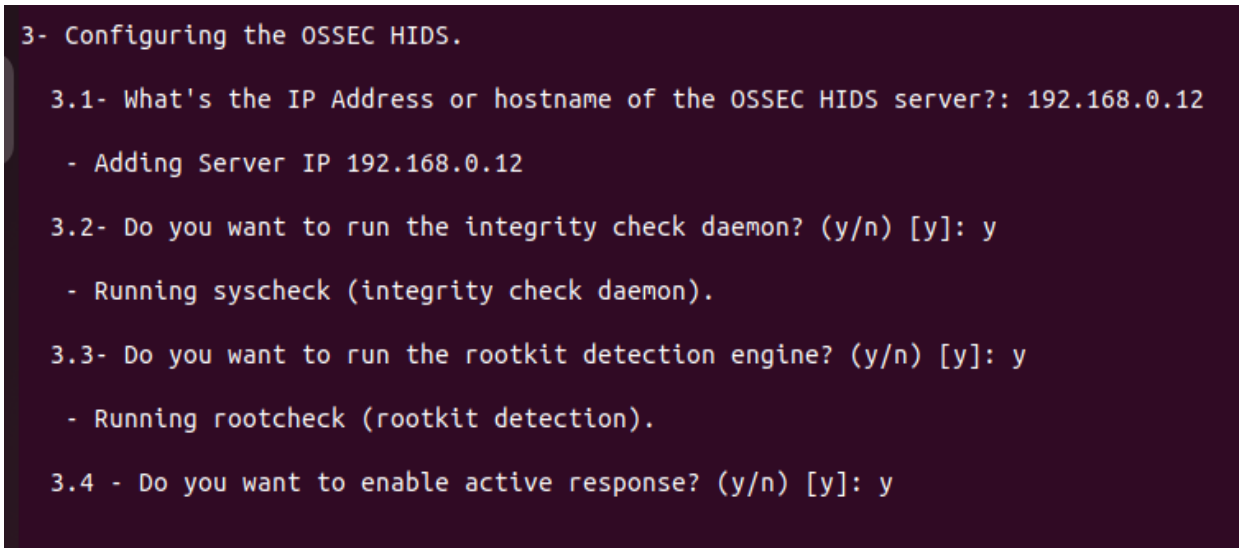
2.3.3.1 Đối với Ubuntu 22.04

Bước 1: Nhìn chung quá trình triển khai trên OSSEC trên các Agent cũng tương tự như trên OSSEC Server không có gì thay đổi, chỉ khác ở chỗ chọn kiểu hoạt động.



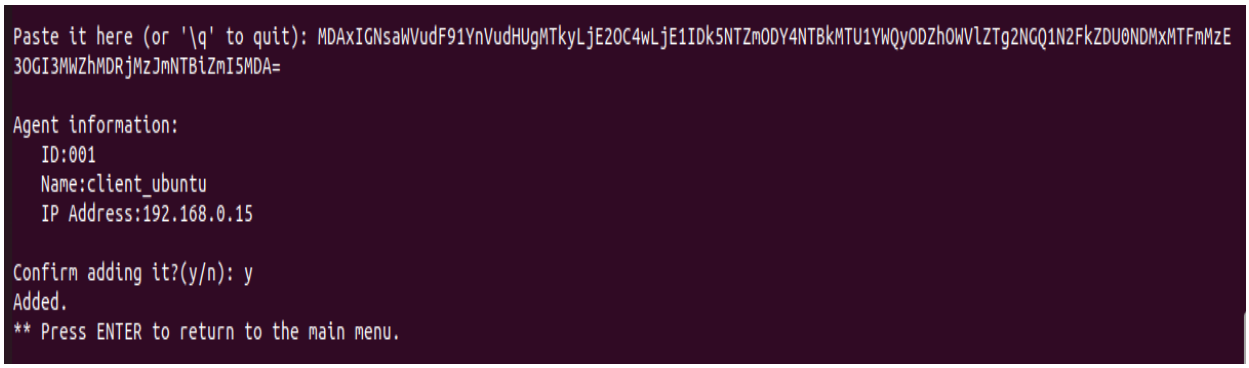
Hình 18 - Chọn chế độ hoạt động Agent

Bước 2: Nhập địa chỉ ip của máy Ossec server và thiết lập như hình sau



Hình 19 - Khai báo địa chỉ IP của OSSEC Server và cấu hình

Bước 3: Sau khi quá trình cài đặt kết thúc, trước khi chúng ta khởi động OSSEC trên Agent bằng câu lệnh: sudo /var/ossec/bin/manage_agents. Chọn I và nhập key xác thực Agent mà Server đã cấp khi thêm Agent ở Server



Hình 20 - Kích hoạt key xác thực đối trên Agent

2.3.3.2 Đối với Windows 7

Bước 1: Đối với hệ điều hành Windown thì chúng ta có thể download OSSEC tại địa chỉ: https://updates.atomicorp.com/channels/atomic/windows/ossec-agent-win32-3.6.0-12032.exe

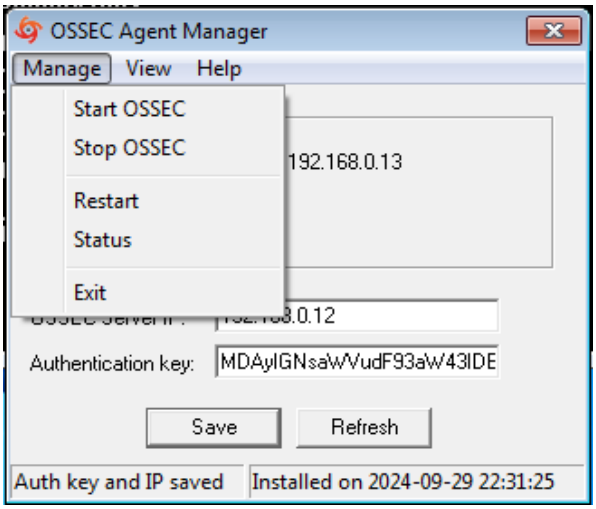
Bước 2: Sau đó tiến hành cài đặt như các phần mềm bình thường khác, quá trình tạo lập trên Server và xác thực tương tự như đối với hệ điều hành linux.

Hình 21 - Giao diện OSSEC

Thực hiện Add Agent vào OSSEC Server cũng tương tự như khi Add hệ điều hành Linux, cũng bắt đầu từ bước Add thêm một Agent mới vào OSSEC Server, tạo key nạp cho client mới (trường hợp này là client Windows), lấy cái key đó nhập vào Agent trên Windows.

Hình 22 - Nhập IP server và key

Chọn Start để khởi động Ossec agent:



Hình 23 - Khởi động dịch vụ OSSEC

Kiểm tra trên Ossec Server:

```
root@ubuntu22:~# sudo /var/ossec/bin/list_agents -c
client_win7-192.168.0.13 is active.
client_ubuntu-192.168.0.15 is active.
```

Hình 24 - Kiểm tra trên OSSEC Server

2.4 Tạo luật trong OSSEC

2.4.1 Luật trong OSSEC

Luật trong OSSEC là những quy tắc được định nghĩa sẵn hoặc do người dùng tự tạo để hệ thống có thể phát hiện các hoạt động bất thường, tiềm ẩn nguy cơ tấn công hoặc vi phạm chính sách bảo mật. Khi một sự kiện trùng khớp với một luật nào đó, OSSEC sẽ gửi thông báo cảnh báo đến người quản trị.

2.4.2 Tại sao luật lại quan trọng?

- Phát hiện sớm mối đe dọa: luật giúp OSSEC phát hiện các hoạt động đáng ngờ ngay khi chúng xảy ra, từ đó cho phép bạn nhanh chóng ứng phó.
- Tùy chỉnh hệ thống: có thể tạo các luật phù hợp với môi trường và nhu cầu cụ thể của hệ thống mình.
- Cải thiện hiệu suất: các luật được tinh chỉnh sẽ giúp giảm thiểu số lượng cảnh báo giả, giúp bạn tập trung vào những mối đe dọa thực sự.

2.4.3 Các loại luật trong OSSEC

- Luật mặc định: OSSEC cung cấp một bộ luật mặc định để phát hiện các hoạt động thông thường như:
  - Thay đổi file hệ thống quan trọng
  - Tạo tài khoản mới
  - Thực thi các lệnh nguy hiểm
  - ...
- Luật tùy chỉnh: Bạn có thể tạo các luật tùy chỉnh để phát hiện các hoạt động cụ thể liên quan đến ứng dụng, dịch vụ hoặc quy trình đặc biệt trong hệ thống của bạn.

2.4.4 Phân loại quy tắc

Các quy tắc được phân loại theo nhiều cấp độ. Từ mức thấp nhất (00) đến mức tối đa 15. Một số cấp độ không được sử dụng ngay bây giờ. Các cấp độ khác có thể được thêm vào giữa chúng hoặc sau chúng.

Các quy tắc sẽ được đọc từ mức cao nhất đến mức thấp nhất.

- 00 – Ignored (Không có hành động nào được thực hiện): Được sử dụng để tránh cảnh báo sai. Các quy tắc này được quét trước tất cả các quy tắc khác
- 01 - None (Không có)
- 02 - System low priority notification (Hệ thống thông báo ưu tiên thấp): Thông báo hệ thống hoặc thông báo trạng thái. Không có sự liên quan đến bảo mật.
- 03 - Successful/Authorized events (Sự kiện thành công/được ủy quyền): Bao gồm các lần đăng nhập thành công, tường lửa cho phép sự kiện, v.v.
- 04 - System low priority error (Lỗi ưu tiên hệ thống thấp): Các lỗi liên quan đến cấu hình hoặc thiết bị/ứng dụng không sử dụng.
- 05 - User generated error (Lỗi do người dùng tạo): Bao gồm mật khẩu bị bỏ lỡ, hành động bị từ chối, … . Không có sự liên quan về bảo mật.
- 06 - Low relevance attack (Tấn công mức độ liên quan thấp): **sâu (worm)** hoặc **virus** không ảnh hưởng đến hệ thống, chẳng hạn như mã độc "Code Red" trên máy chủ Apache, hoặc các sự kiện từ hệ thống phát hiện xâm nhập (IDS) hoặc lỗi thường xuyên
- 07 - "Bad word" matching: để theo dõi và phát hiện các từ ngữ không phù hợp, hành vi đáng ngờ hoặc các chuỗi thường liên quan đến tấn công hoặc vi phạm bảo mật.
- 08 - First time seen: Bao gồm các sự kiện lần đầu tiên được xem. Lần đầu tiên một sự kiện IDS được kích hoạt hoặc lần đầu tiên người dùng đăng nhập.
- 09 - Error from invalid source (Lỗi từ nguồn không hợp lệ): Bao gồm các lần đăng nhập dưới dạng người dùng không xác định hoặc từ nguồn không hợp lệ.
- 10 - Multiple user generated errors (Tập hợp lỗi do người dùng tạo): Bao gồm nhiều mật khẩu không hợp lệ, nhiều lần đăng nhập không thành công, ...
- 11 - Integrity checking warning (Cảnh báo kiểm tra tính toàn vẹn): Bao gồm các thông báo liên quan đến việc sửa đổi các tệp nhị phân hoặc sự hiện diện của rootkit (bằng kiểm tra root).
- 12 - High importancy event (Sự kiện quan trọng cao): Bao gồm các thông báo lỗi hoặc cảnh báo từ hệ thống, hạt nhân, … có thể chỉ ra một cuộc tấn công chống lại một ứng dụng cụ thể.
- 13 - Unusual error (Mức độ quan trọng cao): Lỗi bất thường, hầu hết các lần khớp với một kiểu tấn công chung.
- 14 - High importance security event (Sự kiện bảo mật quan trọng cao): Hầu hết thời gian được thực hiện với sự tương quan và nó chỉ ra một cuộc tấn công.
- 15 - Severe attack (Tấn công nghiêm trọng): Cần chú ý ngay lập tức

2.4.5 Quy trình xử lý luật (rule) trong OSSEC

2.4.5.1 Event (Sự kiện)

- Khái niệm: đây là dữ liệu đào vào mà OSSEC nhận được từ các nguồn khác nhau. Một "sự kiện" có thể là một dòng log từ hệ điều hành, máy chủ ứng dụng, hệ thống mạng, hoặc tệp nhật ký bất kỳ.
- Ví dụ:
  - Dòng log từ hệ thống tường lửa ghi nhận một kết nối từ hệ thống bị từ chối

- Một truy cập trái phép trên máy chủ web
- Mục đích: thu thập dữ liệu thô để phân tích và phát hiện các hành vi bất thường.

2.4.5.2 Pre-decoding (Tiền giải mã)

- Khái niệm: đây là bước chuẩn bị ban đầu, nơi dữ liệu thô được OSSEC phân loại và chuẩn hóa để chuyển sang bước xử lý xâu hơn
- Hoạt động chính:
- Xác định nguồn của log (ví dụ: Apache, Nginx, SSH, hệ thống)
- Loại bỏ các dữ liệu không cần thiết hoặc bổ sung thông tin nhận diện (ví dụ: gắn nhãn log với địa chỉ IP nguồn)
- Ví dụ:
- Từ một log như:

```
192.168.0.1 - - [19/Nov/2024:12:34:56 +0000] "GET /index.html HTTP/1.1" 200 512
```

- OSSEC xác định đây là log từ máy chủ Apache và chuẩn bị cho bước giải mã

2.4.5.3 Decoding (Giải mã)

- Khái niệm: quá trình dịch log thành các trường thông tin có cấu trúc để hệ thống có thể dễ dàng phân tích.
- Hoạt động chính
- Sử dụng các "Decoders" để phân tích dữ liệu theo mẫu xác định trước
- Trích xuất các trường như: thời gian, địa chỉ IP, người dùng, hành động
- Ví dụ: Từ log Apache ở trên, giải mã ra các trường
- Time: 19/Nov/2024:12:34:56
- IP: 192.168.0.1
- Request: GET /index.html
- Status Code: 200
- Kết quả: Log thô trở thành một bản ghi có cấu trúc mà hệ thống có thể so sánh với các luật.

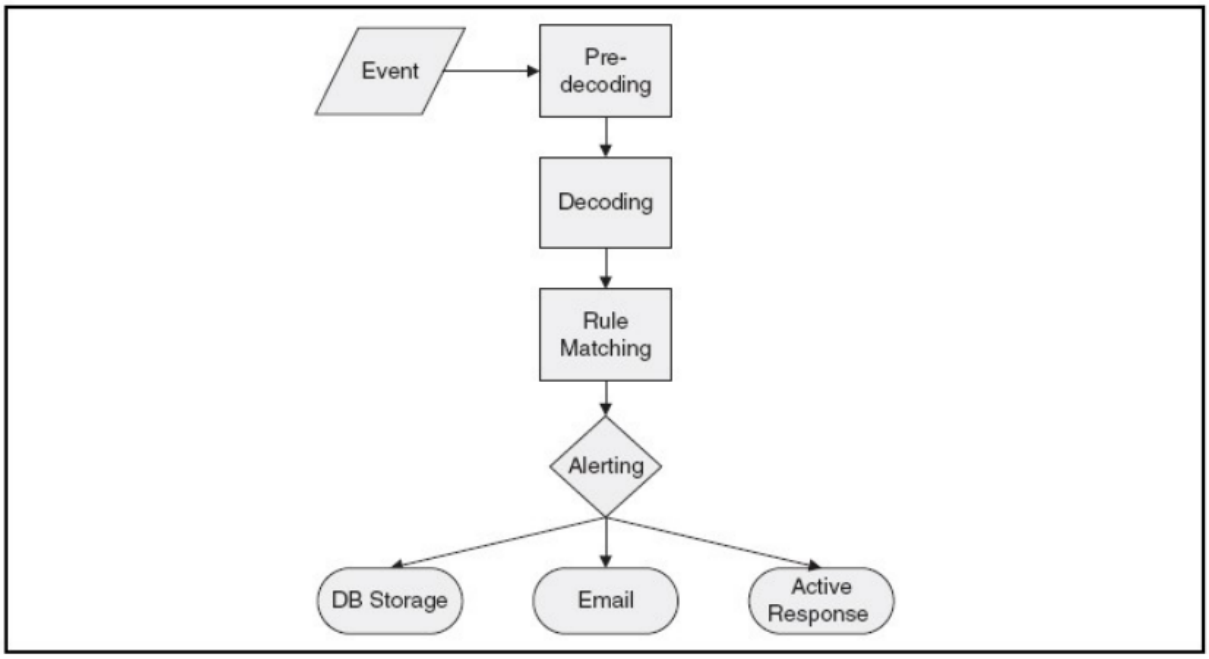
2.4.5.4 Rule Matching (So khớp luật):

- Khái niệm: Sau khi giải mã, OSSEC kiểm tra log dựa trên các tập luật được cấu hình sẵn để phát hiện các sự kiện bất thường
- Hoạt động chính:
- So khớp log với các mẫu luật xác định hành vi cụ thể (ví dụ: dò quét cổng, đăng nhập thất bại nhiều lần, truy cập vào tài nguyên cấm...).
- Mỗi luật trong OSSEC có ID riêng và thường đi kèm với các mức độ cảnh báo
- Ví dụ: Một luật có thể quy định: "Nếu một địa chỉ IP cố gắng đăng nhập thất bại hơn 5 lần trong 1 phút, cảnh báo".
- Kết quả: Nếu log khớp với một luật, hệ thống sẽ kích hoạt cảnh báo.

2.4.5.5 Alerting (Cảnh báo)

- Khái niệm: Khi một log khớp với một luật, OSSEC sẽ đưa ra cảnh báo và thực hiện các hành động được chỉ định.
- Các hoạt động chính
- DB Storage (Lưu trữ cơ sở dữ liệu): Lưu thông tin sự kiện vào cơ sở dữ liệu để phục vụ việc phân tích và kiểm tra sau này.
- Email: Gửi email thông báo tới người quản trị khi có sự kiện bất thường.
- Active Response (Phản ứng chủ động): OSSEC thực hiện các hành động tự động để ngăn chặn mối đe dọa.

- Mục đích: Phản hồi nhanh chóng và giảm thiểu thiệt hại từ các mối đe dọa.



Hình 25 – Quy trình xử lý luật trong OSSEC

2.4.6 Cách tạo luật trong OSSEC

SSEC sử dụng các luật để xác định các mẫu (patterns) trong dữ liệu nhật ký và phản ứng lại các sự kiện bảo mật. Các luật này được định nghĩa trong các tệp XML nằm trong thư mục cấu hình luật của OSSEC. Dưới đây là hướng dẫn cơ bản để tạo luật mới trong OSSEC.

2.4.6.1 Xác định tệp luật

- Luật trong OSSEC được viết bằng định dạng XML có đuôi `.xml` và được lưu trong file:

  `ossec.conf`

- Các tệp luật của OSSEC thường nằm trong thư mục:

  `/var/ossec/rules/`

2.4.6.2 Cấu trúc của luật

Một luật OSSEC thường có cấu trúc như sau:

```
<rule id="100001" level="7">
  <decoded_as>syslog</decoded_as>  <!-- Loại nhật ký -->
  <group>authentication_failed</group> <!-- Nhóm của sự kiện -->
  <description>Failed SSH login attempt</description> <!-- Mô tả luật -->
  <match>Failed password</match> <!-- Chuỗi mẫu để tìm -->
  <regex>sshd\[.*\]: Failed password for .* from (.*) port</regex>
<!-- Biểu thức chính quy -->
  <options>no_full_log</options> <!-- Tùy chọn bổ sung -->
</rule>
```

2.4.6.3 Các phần quan trọng của luật

- **ID của luật** (*id*): Mỗi luật phải có một ID duy nhất. ID này phải nằm ngoài phạm vi ID được OSSEC sử dụng mặc định (thường là từ 100000 trở lên cho các luật tùy chỉnh).
- **Level** (*level*): Mức độ nghiêm trọng của sự kiện. Mức độ này sẽ quyết định loại cảnh báo được tạo ra. Mức độ có thể từ 0 đến 15, với 15 là mức nghiêm trọng nhất.
- **Decoded as** (*decoded_as*): Cho biết loại nhật ký nào mà luật này sẽ áp dụng. Ví dụ: *syslog*, *apache*, hoặc *windows*.
- **Group** (*group*): Nhóm của sự kiện bảo mật, ví dụ *authentication_failed*.
- **Description (***description***)**: Mô tả ngắn gọn về luật để giải thích sự kiện mà nó đang giám sát.
- **Match** (*match***)**: Một chuỗi cụ thể mà OSSEC tìm kiếm trong nhật ký.
- **Regex** (*regex*): Biểu thức chính quy để xác định một sự kiện cụ thể. Điều này rất hữu ích khi chuỗi nhật ký có cấu trúc phức tạp.
- **Options** (*options*): Các tùy chọn bổ sung, chẳng hạn như *no_full_log* để không lưu trữ toàn bộ nội dung nhật ký.

2.4.6.4 Thêm luật mới

Ví dụ, tạo một luật để phát hiện nỗ lực đăng nhập SSH thất bại:

1. Mở tệp luật tuỳ chỉnh (nếu chưa có thì tạo mới):
   ```
   sudo nano /var/ossec/rules/local_rules.xml
   ```
2. Thêm đoạn XML luật mới:
   ```
   <rule id="100002" level="10">
     <decoded_as>syslog</decoded_as>
     <group>authentication_failed</group>
   <description>Failed SSH login attempt</description>
     <match>Failed password</match>
     <regex>sshd\[.*\]: Failed password for .* from (.*) port</regex>
     <options>no_full_log</options>
   </rule>
   ```
3. Lưu lại và thoát.

a) Khởi động lại OSSEC để áp dụng luật

Sau khi thêm hoặc chỉnh sửa luật, bạn cần khởi động lại dịch vụ OSSEC để áp dụng những thay đổi:

```
sudo systemctl restart ossec
```

b) Kiểm tra hoạt động của luật

Sau khi khởi động lại, bạn có thể kiểm tra nhật ký cảnh báo OSSEC để xem luật mới có hoạt động hay không:

```
tail -f /var/ossec/logs/alerts/alerts.log
```

Nếu có bất kỳ nỗ lực đăng nhập SSH thất bại nào, luật sẽ tạo cảnh báo tương ứng.

Lưu ý

- Đảm bảo rằng ID của luật không trùng lặp với bất kỳ ID luật nào đã có trước đó.
- Viết các biểu thức chính quy (regex) cẩn thận để đảm bảo OSSEC có thể phát hiện chính xác sự kiện mong muốn.

2.5 Kết chương

Chương này khái quát về OSSEC là một công cụ mã nguồn mở mạnh mẽ để phát hiện xâm nhập và giám sát an ninh hệ thống. Với kiến trúc client-server gồm agent, server và các module, OSSEC giúp thu thập và phân tích dữ liệu. Cài đặt và cấu hình đơn giản, phù hợp trên nhiều hệ điều hành, cho phép tùy chỉnh qua `ossec.conf`. Tạo luật trong OSSEC giúp giám sát hiệu quả và phản ứng nhanh với mối đe dọa. Tổng kết, OSSEC cung cấp khả năng bảo vệ linh hoạt và đáng tin cậy cho hệ thống mạng.

CHƯƠNG 3. XÂY DỰNG 3 KỊCH BẢN PHÁT HIỆN TẤN CÔNG

3.1 Kịch bản tấn công Brute-Force

3.1.1 Mô tả tấn công:

Brute-force là một phương pháp tấn công trong đó kẻ tấn công thử nhiều tên đăng nhập và mật khẩu khác nhau cho đến khi tìm được một kết hợp đúng để truy cập hệ thống.

3.1.2 Phát hiện bằng OSSEC:

- OSSEC có thể phát hiện brute-force qua việc giám sát các log đăng nhập thất bại từ các dịch vụ như SSH, FTP, hoặc RDP trên Windows.
- OSSEC sử dụng các quy tắc để theo dõi tần suất các sự kiện đăng nhập không thành công. Nếu số lần đăng nhập không thành công vượt qua một ngưỡng nhất định, OSSEC sẽ gửi cảnh báo.

3.1.3 Kịch bản tấn công:

- Cấu hình phản ứng chủ động OSSEC ở file OSSEC.conf trong đường dẫn */var/OSSEC/etc/* như sau:

```
<active-response>
  <!-- Firewall Drop response. Block the IP for
     - 600 seconds on the firewall (iptables,
     - ipfilter, etc).
    -->
  <command>firewall-drop</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>
```

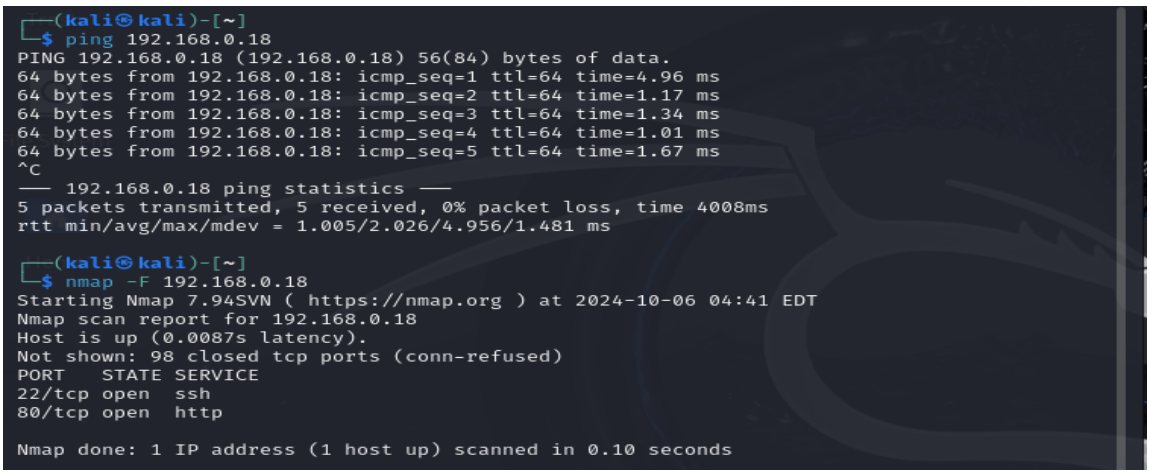
Hình 26 - Cấu hình Active-response trên OSSEC Server

- Sau đó chúng ta phải cấu hình để nhận nhật ký phản ứng chủ động từ các agent, để khi có phát sinh tấn công trên agent thì OSSEC Server sẽ nhận được ngay. Ta sẽ cấu hình *agent.conf* trên OSSEC_Server như sau:

```
<agent_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>
</agent_config>
```

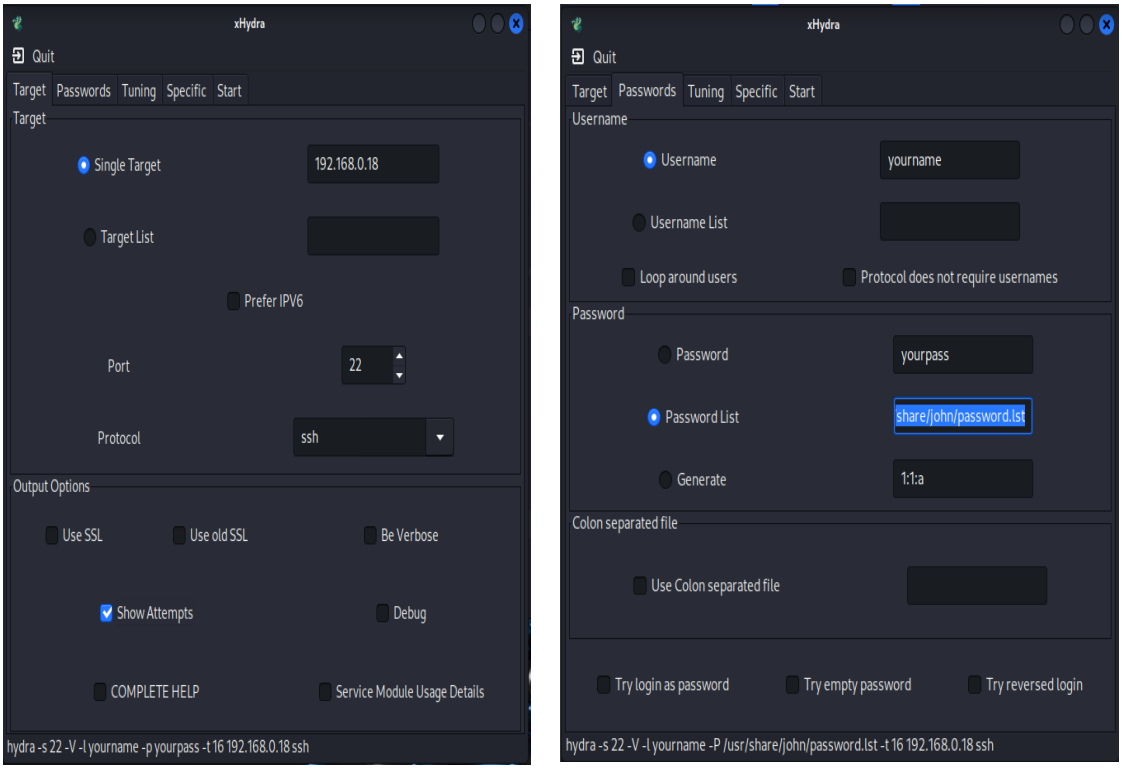
Hình 27 - Cấu hình agent.conf trên OSSEC_Server

- Trên máy Kali Linux (192.168.0.14) chúng sẽ thử ping và quét nmap đến địa chỉ IP của máy OSSEC Agent (192.168.0.18):



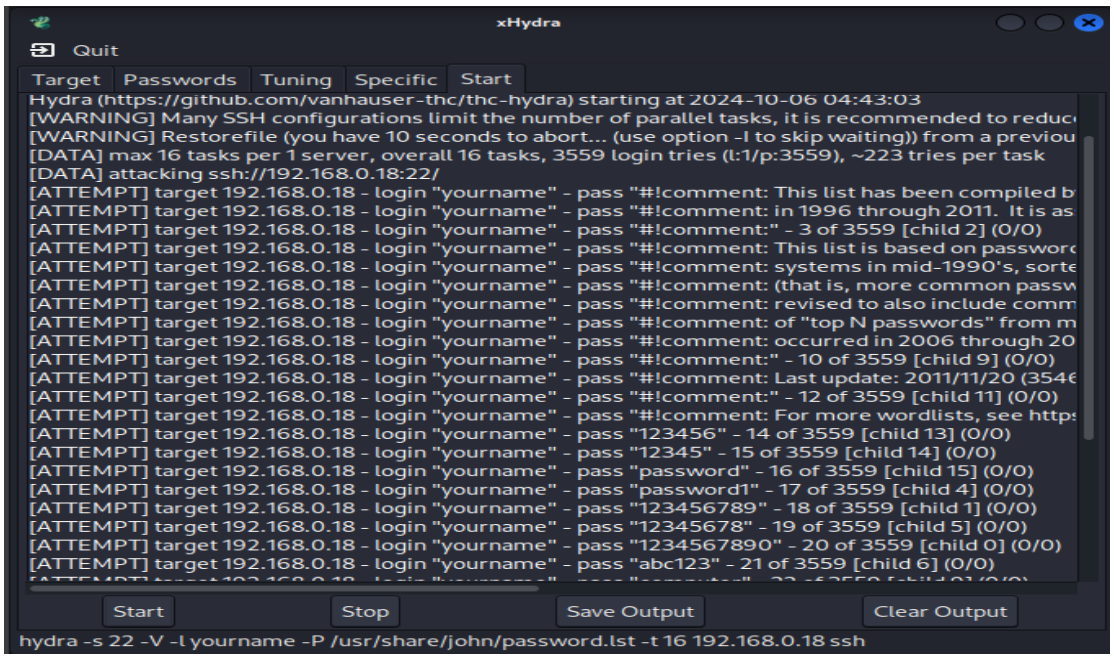
Hình 28 - Attacker lấy được thông tin đăng nhập SSH khi OSSEC không hoạt động

- Port22 SSH đang mở, sử dụng tool xHydra trên Kali Linux để tấn công:



Hình 29 - Sử dụng xHydra trên Kali Linux để tấn công Buteforce SSH

- Chọn Start để quá trình tấn công diễn ra:



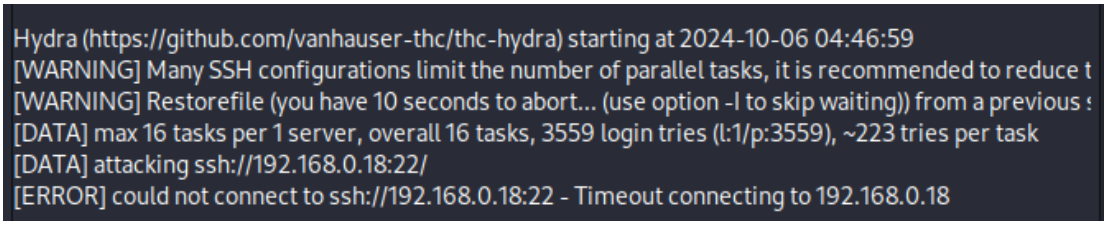
Hình 30 - Quá trình tấn công Buteforce SSH diễn ra

- Trên OSSEC Server phát đi các cảnh báo đăng nhập ssh vào máy client từ IP 192.168.0.14 (kali linux):

```
.168.0.14
Oct  6 15:43:14 ubuntuclient sshd[5151]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
.168.0.14

** Alert 1728204197.22350: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5148]: Failed password for invalid user yourname from 192.168.0.14 port 43620 ssh2

** Alert 1728204197.22705: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5147]: Failed password for invalid user yourname from 192.168.0.14 port 43618 ssh2

** Alert 1728204197.23060: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5146]: Failed password for invalid user yourname from 192.168.0.14 port 43602 ssh2

** Alert 1728204197.23415: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5145]: Failed password for invalid user yourname from 192.168.0.14 port 43600 ssh2

** Alert 1728204197.23770: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5144]: Failed password for invalid user yourname from 192.168.0.14 port 43598 ssh2

** Alert 1728204197.24125: - syslog,sshd,invalid_login,authentication_failed,
2024 Oct 06 15:43:17 (Ubuntu_client) 192.168.0.18->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 192.168.0.14
Oct  6 15:43:16 ubuntuclient sshd[5152]: Failed password for invalid user yourname from 192.168.0.14 port 43638 ssh2
```

Hình 31 - Cảnh báo phát hiện tấn công Buteforce SSH

- Thực hiện tấn công một lần nữa, lần này máy Kali không thể kết nối đến máy nạn nhân:



Hình 32 - Tấn công Buteforce SSH thất bại

- Nguyên nhân là do IP 192.168.0.14 bị chặn bởi TCP Wrappers:

Hình 33 - IP Attacker bị chặn bởi TCP Wrappers

3.2 Kịch bản tấn công Port Scanning

3.2.1 Mô tả tấn công:

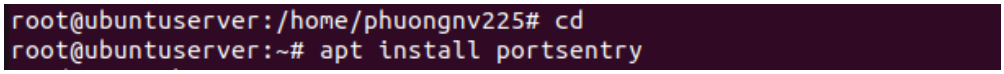
Port scanning là quá trình kẻ tấn công dò tìm các cổng mở trên máy chủ để xác định dịch vụ nào đang chạy và có thể bị khai thác.

3.2.2 Phát hiện bằng OSSEC:

- OSSEC phát hiện port scanning qua việc theo dõi các kết nối đến từ một địa chỉ IP cụ thể trong một khoảng thời gian ngắn tới nhiều cổng khác nhau.
- OSSEC có thể kết hợp với các công cụ mạng như Portsentry để ghi log các sự kiện liên quan đến quét cổng.

3.2.3 Kịch bản tấn công:

- Sử dụng câu lệnh: *apt install portsentry* để cài đặt Portsentry



Hình 34 - Cài đặt portsentry

- Tiếp theo chúng ta cần tạo bộ giải mã để thực hiện trích xuất các thông tin mà portsentry thu được từ file nhật kí hoạt động của nó như địa chỉ IP nguồn, IP đích, các cổng mà hacker đã quét qua trước khi chuyển cho các quy tắc xử lý:

```
<!-- Portsentry -->

<decoder name="portsentry">
  <program_name>^portsentry</program_name>
</decoder>

<decoder name="portsentry-attackalert">
  <parent>portsentry</parent>
  <prematch>attackalert: TCP SYN/Normal scan from host: </prematch>
  <regex offset="after_prematch">(S+)/S+ to (S+) port: (d+)$</regex>
  <order>srcip,protocol,dstport</order>
</decoder>

<decoder name="portsentry-blocked">
  <parent>portsentry</parent>
  <prematch>is already blocked Ignoring$</prematch>
  <regex>Host: (S+)/S+ is</regex>
  <order>srcip</order>
</decoder>

<decoder name="portsentry-scan">
  <parent>portsentry</parent>
  <prematch>^attackalert: </prematch>
  <regex offset="after_prematch">scan from host: (S+)/S+ to S+ port: (d+)$</regex>
  <order>srcip, dstport</order>
</decoder>

<decoder name="portsentry-host">
  <parent>portsentry</parent>
  <prematch offset="after_parent">^attackalert: Host: </prematch>
  <regex offset="after_prematch">^(S+)/S+ </regex>
  <order>srcip</order>
</decoder>
```

Hình 35 - Cấu hình portsentry

- Các quy tắc sẽ dựa vào bộ gải mã này để phát hiện và ngăn chặn hành động dò quét cuả hacker bằng cách block IP của hacker, chúng ta sẽ soạn quy tắc cho OSSEC thực hiện điều này trong file local_rules.xml ở đường dẫn /var/OSSEC/rules như sau: *sudo nano /var/ossec/rules/local_rules.xml*

```
<group name="syslog, portsentry, ">
  <rule id="160000" level="0" noalert="1">
    <decoded_as>portsentry</decoded_as>
    <description>Grouping for the PortSentry rules</description>
  </rule>
  <rule id="160002" level="7">
    <if_sid>160000</if_sid>
    <match>attackalert:</match>
    <description>Detected PortScans, Host IP is already blocked</description>
  </rule>
</group>
```

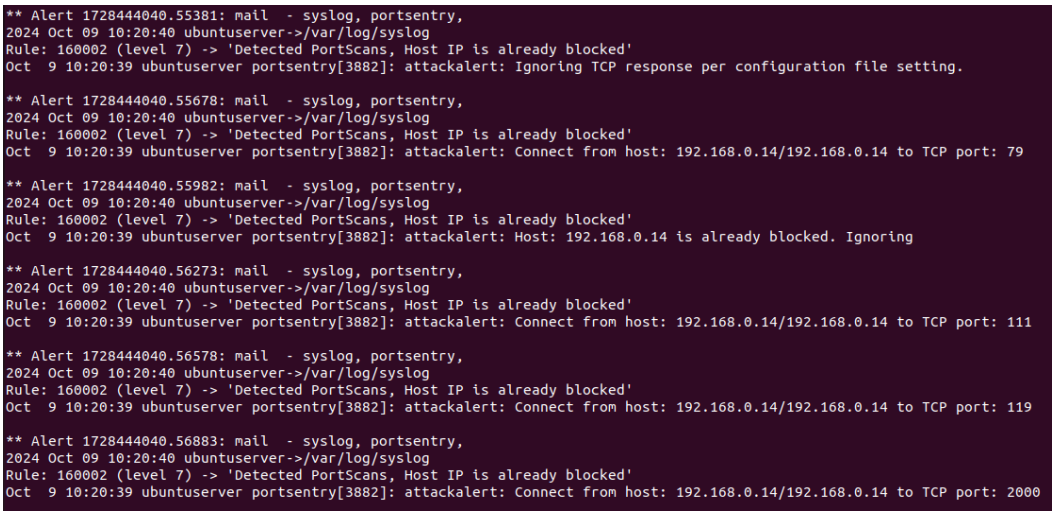
Hình 36 - Tạo local rule trên OSSEC Server

- Sử dụng máy Kali Linux (192.168.0.14) để quét scan port trên OSSEC Server (192.168.0.17) , nếu như OSSEC không hoạt động thì attacker có thể thu được các cổng đang mở của OSSEC Server

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.0.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 23:20 EDT
Nmap scan report for 192.168.0.17
Host is up (0.0060s latency).
Not shown: 94 closed tcp ports (conn-refused)
PORT     STATE SERVICE
79/tcp   open  finger
80/tcp   open  http
111/tcp  open  rpcbind
119/tcp  open  nntp
143/tcp  open  imap
2000/tcp open  cisco-sccp

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Hình 37 - Attacker thu được thông tin cổng khi OSSEC không hoạt động

- Khi OSSEC được bật thì khi hacker có hành động dò quét cổng thì cảnh báo và hành động ngăn chặn từ OSSEC sẽ ngay lập tức được đưa ra. Chúng ta có thể xem các cảnh báo này ở file nhật kí của OSSEC, sử dụng câu lệnh: *cat /var/ossec/logs/alerts/alerts.log* hoặc *tail -f /var/ossec/logs/alerts/alerts.log*



Hình 38 - Cảnh báo phát hiện quét cổng và chặn IP

3.3 Kịch bản tấn công Rootkit

3.3.1 Mô tả tấn công:

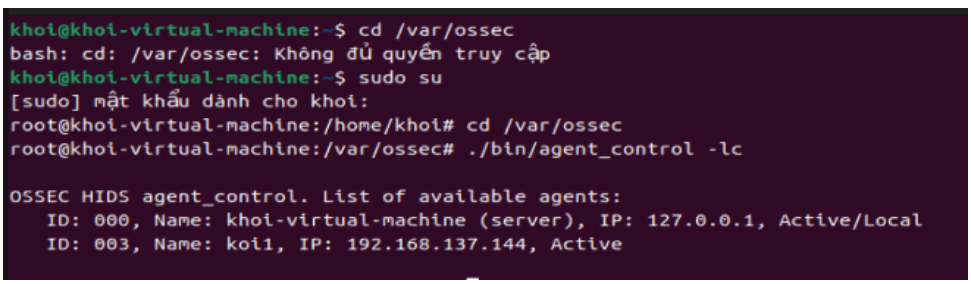
Rootkit là một loại phần mềm độc hại cho phép hacker có quyền kiểm soát hệ thống, thường không bị phát hiện bằng các phương pháp thông thường.

3.3.2 Phát hiện bằng OSSEC:

- OSSEC sử dụng tính năng *file integrity checking* (kiểm tra tính toàn vẹn tệp) để phát hiện rootkit. Nếu một rootkit cố gắng sửa đổi các tệp hệ thống hoặc các tệp nhạy cảm, OSSEC sẽ phát hiện sự thay đổi đó.
- Ngoài ra, OSSEC có thể phát hiện sự bất thường trong các tiến trình hoặc dịch vụ chạy ngầm.

3.3.3 Kịch bản tấn công:

- Trên tệp */var/ossec/* sử dụng câu lệnh *./bin/ agent_control –lc* để xem danh sách các thiết bị Agent

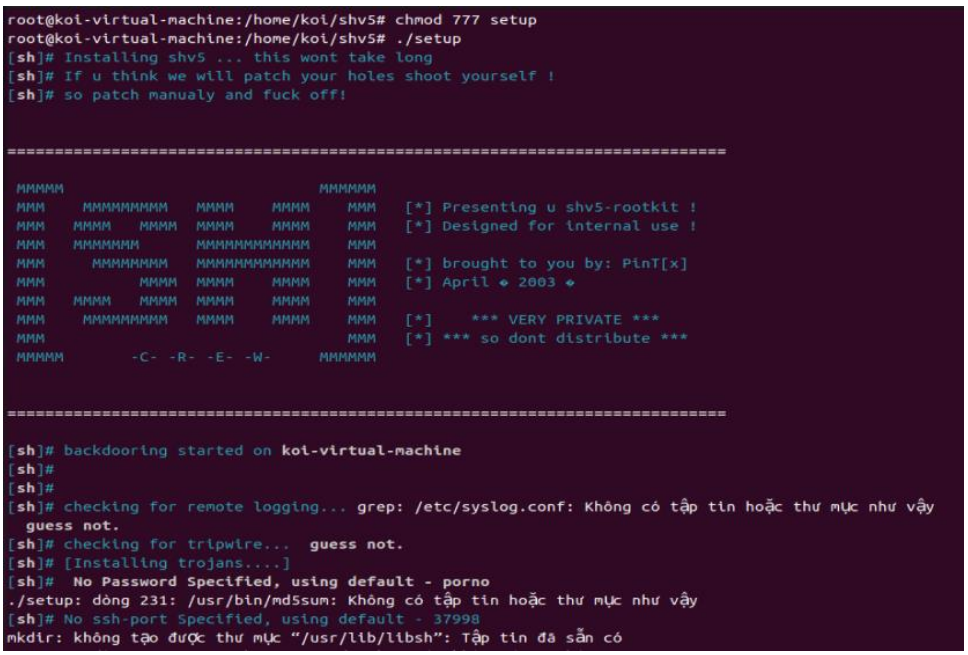


Hình 39 - Danh sách thiết bị Agent

- Trên OSSEC Agent chúng ta sẽ tải SHV5 rootkit qua câu lệnh *git clone* https://github.com/CCrashBandicot/shv5.git

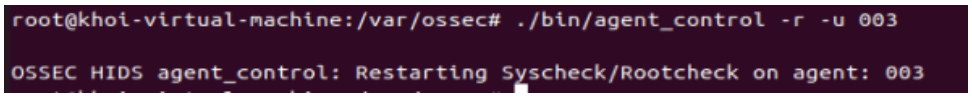
Hình 40 - Tải SHV5 Rootkit từ github

- Trong tệp *shv5* ta sẽ thay đổi quyền truy cập của *setup* qua câu lệnh *chmod 777 setup* và cài đặt *shv5* bằng câu lệnh *./setup*



Hình 41 - Cài đặt Rootkit

- Trên cửa sổ terminal khác của OSSEC Server ta xóa Agent đã cài *shv5* bằng câu lệnh *./bin/agent_control –r –u 003* (003 là ID của Agent)



Hình 42 - Xóa Agnet đã cài shv5

- Trên cửa sổ terminal còn lại của OSSEC Server ta sẽ theo dõi nhật ký để phát hiện các cảnh báo bảo mật, *tail –f logs/alerts/alerts.log*

Hình 43 - Cảnh báo phát hiện Rootkit shv5

3.4 Kết chương

Chương này đã trình bày các kịch bản tấn công và cách OSSEC giúp phát hiện và ngăn chặn chúng:

1. **Brute-Force**: OSSEC phát hiện các cố gắng đăng nhập sai liên tục và có thể khóa tài khoản tự động sau một số lần sai mật khẩu.
2. **Port Scanning**: OSSEC cảnh báo khi có quá nhiều kết nối từ một IP trong thời gian ngắn, giúp phát hiện hành vi quét cổng.
3. **Rootkit**: OSSEC theo dõi sự thay đổi bất thường trong hệ thống, phát hiện rootkit qua kiểm tra tính toàn vẹn của các tệp hệ thống.

Tổng quan, OSSEC giúp bảo vệ hệ thống bằng cách phát hiện và ngăn chặn các mối đe dọa qua các luật cảnh báo và tự động xử lý.

KẾT LUẬN

Các kết quả đạt được

Nhóm thực hiện đề tài "Tìm hiểu về hệ thống phát hiện tấn công, xâm nhập OSSEC" đã hoàn thành việc nghiên cứu, triển khai và thử nghiệm thành công các tính năng cơ bản và nâng cao của OSSEC. Nhóm đã hoàn thành nội dung về kiến trúc, cài đặt, cấu hình và tạo luật của OSSEC.Ngoài ra nhóm đã xây dựng thành công 3 kịch bản phát hiện tấn công: kịch bản tấn công Brute-Force, kịch bản tấn công Port Scanning, kịch bản tấn công Rootkit. Đề tài đã thực hiện đầy đủ các nội dung theo yêu cầu của giảng viên như sau:

- Kiến trúc OSSEC: Đã tìm hiểu về kiến trúc, các thành phần chính cách OSSEC hoạt động.
- Cài đặt và cấu hình OSSEC: Triển khai OSSEC trên cả môi trường máy chủ độc lập và môi trường phân tán để giám sát các hệ thống khác nhau.
- Tạo luật trong OSSEC: Phát triển các luật tùy chỉnh để phát hiện các sự kiện bảo mật phổ biến và phù hợp với các kịch bản cụ thể.
- Xây dựng 3 kịch bản phát hiện tấn công.

Hướng phát triển

Đề tài này có thể được mở rộng theo các hướng sau:

- Tích hợp với các hệt thống khác như: SIEM, hệ thống quản lý sự kiện, phần mềm bảo mật khác....
- Tùy chỉnh và phát triển thêm luật, phát triển thêm các luật cho các kịch bản tấn công trong cái lĩnh vực như giáo dụ, tài chính,....
- Mở rộng khả năng giám sát, phát triển khả năng giám sát nâng cao.
- Cải thiện giao diện và báo cáo, mở rộng môi trường thử nghiệm

TÀI LIỆU THAM KHẢO

[1] https://www.ossec.net/docs/docs/manual/ossec-architecture.html

[2] Rules Classification — OSSEC

[3] UNIX: Active Response Configuration — OSSEC Documentation 1.0 documentation